JITTA

JOURNAL OF INFORMATION TECHNOLOGY THEORY AND APPLICATION

ISSN: 1532-3416

Predator-prey / Obligate Mutualism in Information System Security and Usage

Norman Pendegraft
College of Business and Economics
University of Idaho
norman@uidaho.edu

Abstract:

In this paper, I model the interaction of an information system, its users, and its attackers as an ecological system with three populations. I model the relationship between users and the system as an obligate mutualism and the relationship between the system and the attackers as a predator-prey relationship. Sensitivity analysis on a numerical example suggests that the model is consistent with expectations of economic reality. Critical point analysis suggests that defenses that reduce the reward to attackers are superior to those that reduce damage to assets.

Keywords: Information Security, Ecology, Mutualism, Predator-prey.

Wendy Hui was the Senior Editor for this paper.

1 Introduction

In this paper, I use the idea of an ecological system as an analogy to model information systems under attack. I present two models: 1) a two-dimensional differential equation model and 2) a three-dimensional differential equation model. The first model describes the relationship between an information system (characterized by its value) and its users, and the second describes the relationship between an information system, its users, and a population of attackers.

The notion of an ecology seems highly appropriate if one considers that systems that interact in a variety of ways occupy the Internet. One "subecology" is that of Linux-based (or macOS- or Windows-based) systems. Here, I focus on their economic rather than technical characteristics, but the ecology analogy still holds. Data servers act in a similar way regardless of their technical differences.

One cannot completely solve the proposed model analytically. However, reasonable numerical values for the parameters allow one to make reasonable inferences as to its behavior. Since the proposed models are analytical, they offer several advantages over simulation models.

- They allow one to identify critical points in the state space.
- They allow one to criticize those critical points in terms of the system's behavior in their vicinity.
- They allow one to perform a formal sensitivity analysis of the critical points.

This paper proceeds as follows. In Section 2, I discuss some relevant literature. In Section 3, I present the two-dimensional model and analyze it. In Section 4, I present the three-dimensional model and analyze it. Finally, in Section 5, I discuss this study's implications and possibilities for further work.

2 Background

Computer security (information security, infosec, information assurance, IA) is an economically serious issue. Indeed, it has become a major issue at the highest levels of corporate governance (Yadron, 2014). Verizon (2013) examined 47,000 incidents that occurred in 2012, including 621 confirmed data breaches, and concluded that the majority of the attacks were economically motivated and that 19 percent were "perpetrated by state affiliated actors" (p. 4) (i.e., spies). The Internet Crime Complaint Center (2013) reports that, in 2012, U.S. companies suffered 289,874 incidents that cost in excess of US$500 trillion. The Ponemon Institute (2012) notes that cybercrime is very costly to its victims. The Verizon report cited above also notes that the vast majority of the data breaches (78%) involved attack vectors that were of low or very low difficulty. Only one data breach (of 510 rated) was of high difficulty. It appears that one of the major difficulties that businesses have in preparing to deal with cybercrime is lack of resources—financial and human. In a survey with 1836 responding organizations, Ernst & Young (2012) found that 43 percent reported that they lacked people with the correct skills and training to defend their systems and that 62 percent reported that they had budget constraints that limited their abilities to deal with Information security. Thus, how to best allocate those resources is an important managerial concern.

Since many of the problems in computer security are technical, much research in computer security has unsurprisingly focused on technical solutions such as formal methods, access control, intrusion detection, and encryption. Bishop (2003) offers an excellent introduction to these subjects and an extensive bibliography. Herzog, Shahmehri, and Duma (2007) provide an interesting ontology of information security; virtually all of the countermeasures that they identify are technical.

Contribution:

This speculative paper reports models of the interaction between an information system, its users, and attackers. The models use differential equations and builds on an ecology analogy. Although differential equations and the ideas of ecology have recently been used in the information assurance literature, both remain novel. To demonstrate external validity, I show that the model is consistent with some expected behaviors. Analysis of the critical points suggests that policies to actively reduce the number of attackers or to reduce their rewards from their attacks are more valuable than passive defenses. This result suggests that better law enforcement is an essential part of the solution that requires the ability to identify attackers, which is currently difficult. Microsoft's recent efforts to address the hot bot fraud (Stewart & Marr, 2014) serves to illustrate this result. The paper may provide a basis for future work on extending the mathematical model or for empirical work on evaluating the parameters. It should be of interest to those interested in the modeling, economics, or simulation of security problems.

The literature does not focus only, however, on technical matters. For instance, as long ago as the 1970s, authors such as Saltzer and Schroeder (1975) noted the importance of "psychological acceptability" in computer security. Several authors have since addressed the impact of technology on user behavior. In particular, researchers using the technology acceptance model, the IS success model, and their successors (Wixom & Todd, 2005; Venkatesh, Morris, Davis, & Davis, 2003; Davis, 1989; DeLone & McLean, 1992) have shown that users' attitudes affect their use of information technology. Novakovic, McGill, and Dixon (2009) used the unified technology acceptance and survey data to examine user behavior and found that usability had a positive effect on users' behavior.

Economics also affects behavior. Becker (1968), in a landmark work, pioneered the use of economic models to study criminal behavior. In particular, he argued that one can understand criminal actions as rational economic decisions. Since then, many others have used economics to examine information security. For example, Gordon and Loeb (2002) developed and applied economic analysis to the problem of information security. They used their model to determine the optimal amount to spend on security while considering the potential loss and vulnerability. Among their interesting results, they found that investing in defending one's most vulnerable targets is not necessarily optimal. Anderson and Moore (2007) surveyed results from the economics of information security and identified several interesting economic issues. They classify them into four themes: designing better systems, general security, dependability, and the border between economics and psychology. Several authors have used game theory models to examine attacker behavior in security games. While they do not explicitly consider information security, Yang, Kiekintveld, Ordonez, Tambe, & John (2013) summarize that work well. They also use prospect theory to model attacker behavior.

Others have focused on the dynamic character of computer security. Of particular interest here are those authors who have used systems dynamics (Sterman, 2000) to study various aspects of the problem. Dutta and Roy (2008) examine the evolution of system value after security incidents. Behara, Huang, and Hu (2010) develop a model of investment for information security. Rosenfeld, Rus, and Cukier (2007) use system archetypes (Senge, 1990; Braun, 2002) to analyze security scenarios. Pendegraft and Rounds (2007) create a simulation to study the evolution of the value of a system under attack. They assume that attackers and users make rational decisions about system use and attack. In particular, they assume that increased system value attracts users and attackers and that use increases value while attacks decrease value. Their show that the evolution of system value depends on initial conditions and various parameter values. Their model serves as a starting point for the current work.

The general problem I focus on here concerns how to best allocate limited resources to defend the information system (IS). In order to do that, one needs a model of the interactions between the system, the users, and the attackers, which explains why I appeal to ecology for the model. In their classic paper, Hannan and Freeman (1977) propose an ecology model of organizations. They emphasize the selection focus of ecology. Their proposal has spawned a significant literature. Betz and Stevens (2013) discuss the use of analogies (including ecology) in security research. They discuss the strengths, weaknesses, and unstated premises of military, spatial, and biological analogies. They identify several biological analogies used in security discussions, such as viruses, public health, and ecology, and they offer a brief survey of their use. They also discuss the implications of the analogy in public discourse. One advantage is that it is not "martial". They note the difficulty in translating concepts from one field to another. While they acknowledge that some (Thimbleby, Anderson, & Cairns, 1998) find the medical metaphor for viruses misleading, they see no major problems with using the biology metaphor. They note that one advantage of ecology is that it includes both benign and malign components. One can expand such models to include human agents who interact with a system. These reasons seem to more than justify using the ecology analogy.

Sportelli (1994) uses the predator prey model to overcome the structural instability of Goodwin's (1982) growth cycle model. Mehlun, Moene, and Torvik (2003) use a predator prey model to study extortion and similar crimes in developing economies. Tschirhart (2004) points out the similarity between economic equilibrium and stability in a predator-prey ecology. Furnell (2008) makes a good case for the ecology model. In particular, he notes that "predators" have demonstrated an ability to adapt faster than "prey" have. He offers a detailed argument that the "analogy between the biological ecosystem and the Internet is clear" (p. 4). Jorgensen, Rossignol, Takikawa, and Upper (2001) suggest that ecology is a useful way to understand the information assurance problem. Rounds, Pendegraft, and Taylor (2007) explicitly discuss the ecology of information security. Crandall, Ensafi, Forrest, Ladau, and Shebaro (2008) use the ecology paradigm to study malware and treat different types of attacks as different species. Others (Mishra &

Saini, 2007; Mishra & Jha, 2010) use epidemiological ideas to develop differential equation models of malware propagation treating malware as an epidemic disease.

In mathematical ecology, mutualists refers to two species that interact in such a way as to increase each other's population (Brauer & Castillo-Chavez, 2000). When each species can survive without the other, the relationship is called facultative mutualism. When neither party can survive without the other, the relationship is called obligate mutualism. I use the idea of obligate mutualism to model the interaction between an information system and its users. Clearly, if the information system (IS) has no value, it will have no users, and, if it has no users, then the system's value will decline to zero. In this context, data primarily creates value. Of course, some system value resides in the hardware and software infrastructure, but even infrastructure loses value as it becomes obsolete. So the model does not lose validity even if it includes infrastructure.

I looked to the ecology literature for guidance in modeling the interaction between the IS and its users. Addicott (1981) shows that a mutualistic relationship can lead to a stable or an unstable system. Dean (1983) includes external limits in two mutualist populations due to external constraints. In particular, he includes a limit, dependent on the population of the other species, in the logistic growth term of his model. Rai, Freedman, and Addicott (1983) and Addicott and Freedman (1984) study three-species systems with two in a mutualistic relationship and the third the prey of one of the first two. Freedman, Addicott, and Rai (1987) identify four biologically significant ways that mutualists can interact to benefit a third, predator population. One of those—increasing the number of prey—is consistent with our approach here. In addition, they also make assumptions about the signs of some parameters that I cannot use here. Hoeksema and Schwartz (2003) use an economic model of comparative advantage to model mutualism, and McGill (2005) extends their work to explore facultative mutualism. Bronstein (1994) offers a comprehensive survey of biological mutualistic models.

Pirolli and Card (1995) introduced the idea of information foraging. They called on the ecology literature to describe information-seeking behaviors. Subsequently, Pirolli (2009) offered a framework that extends theory about making predictions about behaviors. He did not consider security, but the notion of information as an analogy to food in a biological system is useful here. In extending the information-as-food analogy, I take system value to reside largely in a system's information: for example, in a database or on a social media site.

The literature that deals with biological systems includes characteristics (see Section 3) that I believe are inappropriate for the economic relationship between a system and its users. Thus, I offer here a two population model with a mutualistic relationship tailored to information security.

3 Two-population Model

Since the three population model is complex, I found it useful to initially consider a system with only two species. The two-population model accounts for the interaction between system and users (and attackers) following the standard ecology model (Brauer & Castillo-Chavez, 2000). I follow this model because it is well known and seems to fit the system / user interaction reasonably well. In this paper, among other things, I evaluate the appropriateness of their assumptions. Perhaps my strongest assumption is that species interact proportionately to the product of their populations. Here, I use user population and system value. Other studies address system value's "fuzziness" (Pendegraft & Rounds, 2007).

Ecologically, I characterize the user-system interaction as a mutualism. I make several assumptions that I believe make sense for an IS and its users.

- The system is deterministic.
- One can describe system value with a single variable.
- The system will decline in value if it is not used.
- Use will increase an information system's value.
- If the system value increases (declines) in value, then the rate of use will increase (decrease).
- The system and users interact proportionally to the product of system value times user population.

The standard model for population ecology uses the Kolmogorov model, which follows the following format (Brauer & Castillo-Chavez, 2000):

x' = x F(x,y)

y' = y G(x,y)

I include two terms in both F and G. One term is the growth term (i.e., the natural response of a population ignoring the impact of the other population). In biology, this usually has a positive growth component with some sort of limiting character. The second term is the interaction term; a function of both populations, it is commonly modeled as a product of both populations. This sort of modeling assumes that the populations interact randomly. I acknowledge that this assumption is strong but believe it to be tolerable.

The key difference between this model and that typically found in biological systems is that I assume that neither population has any ability to grow on its own (i.e., $F(x,0)\leq 0$ and $G(0,y)\leq 0$). A second difference resides in the interaction term. While increasing the value of the system will increase the rate at which use increases, it will do so at a decreasing rate. Dean (1983) emphasizes the importance of biologically meaningful ways to limit growth, and I follow his lead by imposing economically meaningful limits on system value and user population. The value of systems is inherently limited by the amount of data that they can store and that data's value. My models differ from Dean's in that I use a rational function with polynomial terms rather than an exponential partly because of its simplicity. The model assumes that system value (V) and user population (U) have natural upper limits, K_v , K_u, due to external factors such as technology and investment. V also has an upper limit, V_{max}, that depends on the current value of U. Since the system has value only because of users, the number of those users must limit its value. I further assume that additional users have decreasing marginal value. Thus V_{max} is a function of U that behaves as Figure 1 shows. In other words, $\frac{\partial \text{Vmax}}{\partial \text{U}}>0$ and $\frac{\partial^2 \text{Vmax}}{\partial \text{U}^2}<0$.

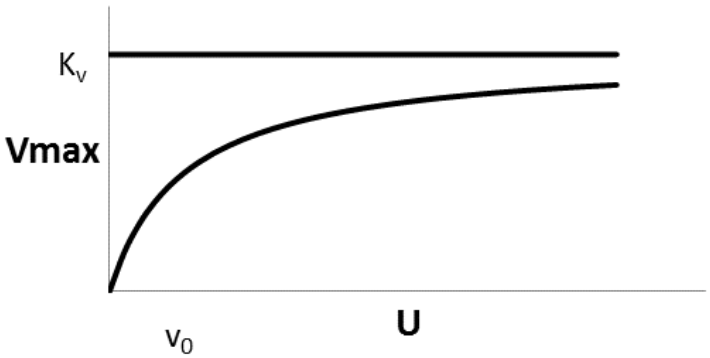


Figure 1. Upper Limit on V as a function of U

A simple way to model the limit is $V_{\max} = \frac{K_v U}{v_0 + U}$. Here, K_v is the maximum limit on V imposed by externalities and v0 is a shape factor that specifies the level of U that gives V_{max} equal to half of K_v. Thus specified, V_{max} satisfies the criteria specified above. That is:

$$\frac{\partial V_{\max}}{\partial U} = \frac{K_v v_0}{(v_0 + U)^2} > 0, and \ \frac{\partial^2 V_{\max}}{\partial^2 U} = \frac{-2K_v v_0}{(v_0 + U)^3} < 0 \quad (1)$$

I use a similar argument to develop U_{max}, the upper limit for U.

The labeling of v0 may seem odd. I use "v" rather than "u" because it is a parameter in the equation that defines V. This labeling will be clearer after examining the model. To clarify the notation, Appendix A presents a table of notation.

3.1 The Model

I model the interaction as follows:

$$\dot{V} = \frac{dV}{dt} = -v_1 \mathrm{V} + v_2 VU\left(1 - \frac{V}{V_{max}}\right) = -v_1 \mathrm{V} + v_2 VU\left(1 - \frac{V(v_0 + U)}{K_v U}\right) \quad (2)$$

$$\dot{U} = \frac{dU}{dt} = -u_1 \mathrm{U} + u_2 VU\left(1 - \frac{U(u_0 + V)}{K_u V}\right) \quad (3)$$

I assume all of the parameters to be positive.

3.2 Model Discussion

Since Equations 1 and 2 are similar, I explain only Equation 2. The first term, $-v_1 V$, represents a loss in system value that naturally occurs due to stale data and technological obsolescence. This term is analogous to the natural death rate in a biological model. The second term $\left(u_2 VU\left(1 - \frac{U(u_0+V)}{K_u V}\right)\right)$ represents the growth in system value due to interaction between the system and the users. V increases at a rate proportional to V and to the amount of usage, U. The change is proportional to the frequency of the interaction between users and the system, which I assume as per the ecology analogy to be proportional to the product of U and V. The more users and the greater the value of the system, the more interactions there will be. The final factor in that term recognizes that the rate at which V increases declines as V increases and that it ultimately falls to 0 as V approaches V_{max}. Equation 3 has a similar interpretation.

The two parameters, v_1 and u_1, represent the rate at which these values decline absent the other population. Similarly, v_2 and u_2 are the "growth" rates. But, they are factors in a term including the product UV, so they imply growth when only U and V are both positive.

Before I solve this system, I consider an illustrative example (I thank the senior editor for the paper for suggesting this example). Consider a social media system. The value of such a system resides largely in its data and features. Modeling its relationship with its users as a mutualism seems very reasonable. There is no use without the system and no system value without users. Note that both have inherent upper limits. In particular, use is limited by the Earth's population, and system value has inherently limited economic value. The more value a system has, the more users it will have and vice versa. The u_1 parameter reflects the rate at which users stop using a system (perhaps in favor of another system), while u_2 reflects the rate at which system value attracts new users. Similarly, v_1 captures the rate at which the system loses value (perhaps due to social media), to fashionable features.

The model assumes that the parameters are constant (at least over some reasonable period of time). But there is no reason to assume that the parameters have the same values for all systems. It is entirely possible that parameters might change, such as when new competing systems are established or when fashions change. As an example, MySpace's demise relative to Facebook (Vascellaro, Steel, & Adams, 2011; Chiemleroski & Sarno, 2009) may have been due to the higher perceived value that Facebook offered or due to changes in the parameters of the MySpace system similar to the increases in v_1 that I examine in Section 3.5 (Case 2).

3.3 Solution

I follow the usual procedure for solving such systems (see, e.g., Boyce & DiPrima, 2005). To evaluate such a system of equations, I first identify the nullclines and critical points. The nullclines are the sets of points where the two time derivatives are 0. That is, on the nullcline, the variable does not change over time. At their points of intersection, the critical points (CP), both variables are constant over time. While the nullclines are not inherently interesting in themselves in this problem, the critical points are. A stable CP is akin to an economic equilibrium point.

At the critical points, the system has some sort of equilibrium, which I evaluate in due course. To determine the nullclines, I set $\dot{U}$ and $\dot{V}$ equal to 0. One can see immediately that V = 0 and U = 0 are nullclines and that there is a critical point at the origin. One can then factor out V from Equation 2 and U from Equation 3, which leaves:

$$-v_1K_v + v_2(K_vU - v_0V - UV) = 0 \tag{4}$$

$$-u_1K_u + u_2(K_uV - u_0U - UV) = 0 \tag{5}$$

One can arrange these equations to get:

$$UV + v_0V - K_vU = -\frac{v_1}{v_2}K_v \tag{6}$$

$$UV + u_0U - K_uV = -\frac{u_1}{u_2}K_u \tag{7}$$

These are both hyperbolas in the U V space. Table 1 provides the asymptotes and intercepts. Equation 8 provides the value of V at the intersections:

$$V^* = \frac{(u_0v_0v_2v_2 + v_2K_uu_1 + K_vK_uu_2v_2 - K_vu_2v_1 + \sqrt{\begin{array}{c}u_0^2v_0^2u_2^2v_2^2 - 2v_2v_0u_2u_0K_uu_1 - 2v_2^2u_2^2u_0K_vK_u - 2v_2^2v_0u_2^2u_0v_1K_v \\ + v_2^2K_u^2u_1^2 - 2v_2^2K_u^2u_1K_vu_2 - 2v_2K_uu_1v_1K_vu_2 + v_2^2K_v^2K_u^2u_2^2 \\ +2v_2K_v^2K_uv_0u_2^2v_1 - v_1^2K_v^2u_2^2 - 4v_2^2v_0u_2K_vK_uu_1 - 4v_1K_uu_2^2u_0v_1K_v\end{array}}}{2(v_2\ v_0\ u_2\ v_2\ K_u\ u_2)} \tag{8}$$

I omit the similar equation for U for brevity. As one can see, Equation 8 is not a convenient expression to evaluate analytically, so I do so mostly with numeric examples. However, one can observe that, when the quantity under the radical is positive, there are two points of intersection and that, when it is negative, the intersections are complex.

Table 1. Nullcline Asymptotes and Intercepts

	Asymptotes		Intercepts	
	$V \to \infty$	$U \to \infty$	U = 0	V = 0
V null cline (5)	$U = -v_0$	$V = K_v$	$V = -K_vv_1/v_0v_2$	v_1/v_2
U null cline (6)	$U = K_u$	$V = -u_0$	$V = u_1/u_2$	$-K_uu_1/u_0u_2$

3.4 Critical Point Evaluation

I chose parameters (Table 2) to illustrate the two-intersection case. Figure 2 shows the general appearance of these curves in the UV phase plane. There are two points of intersection in the positive quadrant. One (farther from the origin) is a coexistence or stable equilibrium (i.e., both populations survive in positive numbers). The second is an unstable equilibrium, which divides the phase plane into two regions: one that evolves toward the origin and another that evolves toward the coexistence point.

To characterize the critical points, I calculate the Jacobian (community) matrix:

$$J = \begin{bmatrix} -v_1 + v_2U - 2v_2\mathrm{V}\left(\frac{v_0 + U}{K_v}\right) & v_2V(1 - \frac{V}{K_v}) \\ u_2U(1 - \frac{U}{K_u}) & -u_1 + u_2\mathrm{V} - 2u_2\mathrm{U}(\frac{u_0 + V}{K_u}) \end{bmatrix} \quad (9)$$

Section 1 in Appendix B provides the code. At the origin:

$$J = \begin{bmatrix} -v_1 & 0 \\ 0 & -u_1 \end{bmatrix} \quad (10)$$

The values of its eigenvectors at the critical points reveal the character of the critical point. As an example, I evaluated the system with the following parameters, which seem to be plausible values at least in relation to one another.

Table 2. Case 1

K_u	K_v	v_0	v_1	v_2	u_0	u_1	u_2
100	300	20	.1	.01	60	.1	.01

Table 3 show the eigenvalues at the critical points (CPs) for Case 1 (section 3 in Appendix B shows the code).

Table 3. Critical Point Evaluation: Case 1

Critical Point (CP)	U*	V*	Eigenvalues		Characteristic	
1	0	0	-.1	-.1	Sink	stable
2	12.1	19.6	.086	-0.203	Saddle point	unstable
3	73.4	203.7	-.54	-2.02	Sink	stable

Since the eigenvalues for the origin are negative, it is stable (i.e., a sink). Systems in its vicinity will gravitate toward it. The eigenvalues of the next CP differ in sign, which means that it is a saddle point. That means that any solutions in the vicinity will move toward that point along one axis but away along the other. Similarly, the third CP is also a stable equilibrium.

The graphs in Figure 2 illustrate the nullclines and phase diagram (see section 4 in Appendix B). One is a close-up of the critical point nearer the origin. The phase diagram confirms the analysis regarding the nature of the critical points.

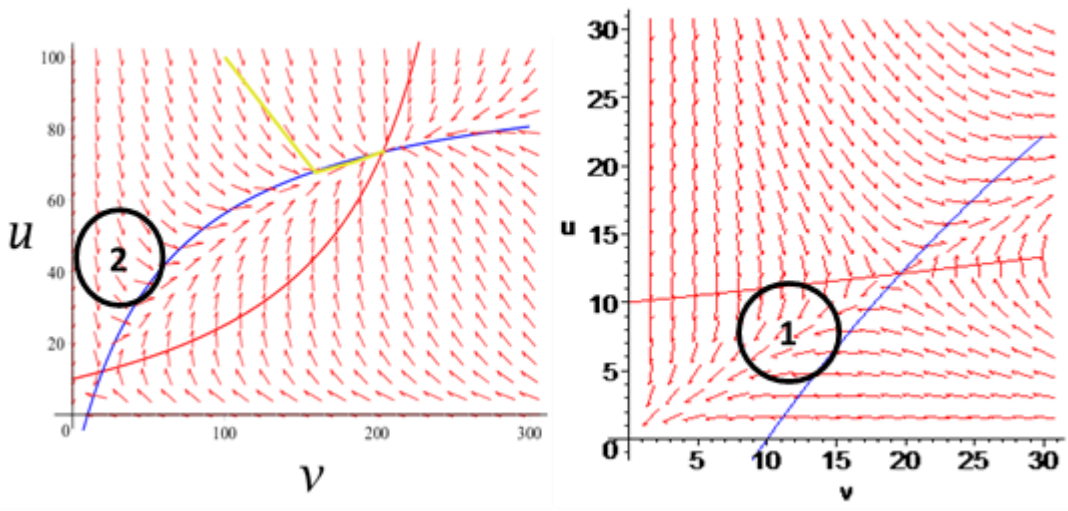


Figure 2. Vector Field for Case 1 (Close-up on Right)

Since the nullclines are hyperbolas, they can intersect in 0, 1, or 2 points. I chose values for the parameters to illustrate the case with zero intersections and the two-intersection case. While they reflect

specific cases, they nonetheless illustrate the range of possible behaviors for the system. Thus, there is nothing "magical" about the parameters I selected. I made some effort to make the values "reasonable" with respect to each other. As the two-intersection case that Figure 2 illustrates, the system will evolve to one of two points (stable CPs). One is at the origin, which is to say that the system has no value and no users. The other is in the positive quadrant, which suggests that there is a stable economically viable solution to the system. Any slight deviation from that CP will result in the system returning to the CP. The ultimate destination of the evolution of a system depends on its initial conditions (i.e., where it starts). The arrows in the phase diagrams indicate in which direction a system in each location will move. In particular, a system starting with a low value (point 1) and a small number of users will become extinct. The clear implication is that, to be viable, a system must have some significant initial value, which makes sense from an economic point of view. If it is to survive, it must be adequately funded with respect to infrastructure. From users' point of view, its content must have some initial intrinsic value or it will not attract sufficient users to survive. In many cases, novelty may attract users (Chau & Hui, 1998). Fashion theory (Sproles, 1974) suggests that novelty in itself may attract consumers. Similarly, an obsolete system with low value (point 2) and many users might evolve in either direction depending on exactly where it is in the state space. Arguably, one could model obsolescence in such a case by changing the value of v_2 (or v_0 or K_u). Since this model has constant parameters, such a change would essentially be a "new" system (I thank a reviewer for suggesting this example).

3.5 Sensitivity Analysis

To illustrate the sensitivity of the CP to changes in the parameters, I slightly varied two of the parameters. In particular, u_1 and v_1 were increased while the other parameters were kept constant (Table 4). In the social media site, these represent the rate at which users abandon a site and the rate at which the site content becomes stale or obsolete due, perhaps, to natural aging or loss of fashionability. Figure 3 shows the evolution of the system as u_1 and v_1 change. (See Appendix B section 5.) The thin solid lines (labeled c1) are the original system (Case 1). The thick dashed lines are the nullclines for Case 2, and the dotted lines are from Case 3. The stable critical point in Case 2 (CP2) is substantially closer to the origin than is the critical point for Case 1 (CP1). As one increases u_1 and v_1 further, the stable equilibrium disappears (Case 3) and the system declines both in value and users to extinction. I do not claim that this explanation fully explains the behavior of these systems, but it does seem to model it.

One could observe such behavior in MySpace after Facebook appeared. News Com purchased MySpace in 2005 for $580 million. By mid-2009, Facebook had more participants, and, in 2011, News Comm sold MySpace for about $35 Million. In the opinion of some, social network sites have "the fleeting popularity of a trendy nightclub" (Chmieleski & Sarno, 2009). They and others (Digital Trends Staff, 2014) suggest that Facebook's better innovation allowed it to overtake MySpace.

Consider also the case of another social media site, Friendster. It pioneered social media, but is now defunct. It reappeared as a gaming site in 2011 but shut down in 2015 (Friendster.com). In studying Friendster's rapid decline, Garcia, Mavrodiev, and Schweitzer (2013) conclude that changes in a website may cause users to leave, which, in turn, causes others to leave and so on. If many users have only a handful friends, a website may be vulnerable to a rapid decline such as Friendster's. That situation might correspond to a high v_1 value and low u_2 and v_2 values. Their study may provide hints for how to evaluate the parameters in the current model, but I do not do so here. A possible policy implication of their study and the two population model offered here is that website managers should monitor the rate at which users stop using the system and survey changes in customer satisfaction, the results of which they could use to estimate v_1 and u_1, respectively.

I continue the sensitivity analysis by briefly examining the impact of the parameters individually on the solution's geometry. Figure 4 illustrates the impact of change to u_0 (see section 5 in Appendix B). Note that, as u_0 increases to near 300, a behavior change occurs, and the system no longer has real critical points other than the origin. Changes in the values of the other parameters have similar results.

Table 4. Sensitivity Analysis Cases

	K_u	K_v	v_0	v_1	v_2	u_0	u_1	u_2
Case 1	100	300	20	.1	.01	60	.1	.01
Case 2	100	300	20	.2	.01	60	.2	.01
Case 3	100	300	20	.3	.01	60	.3	.01

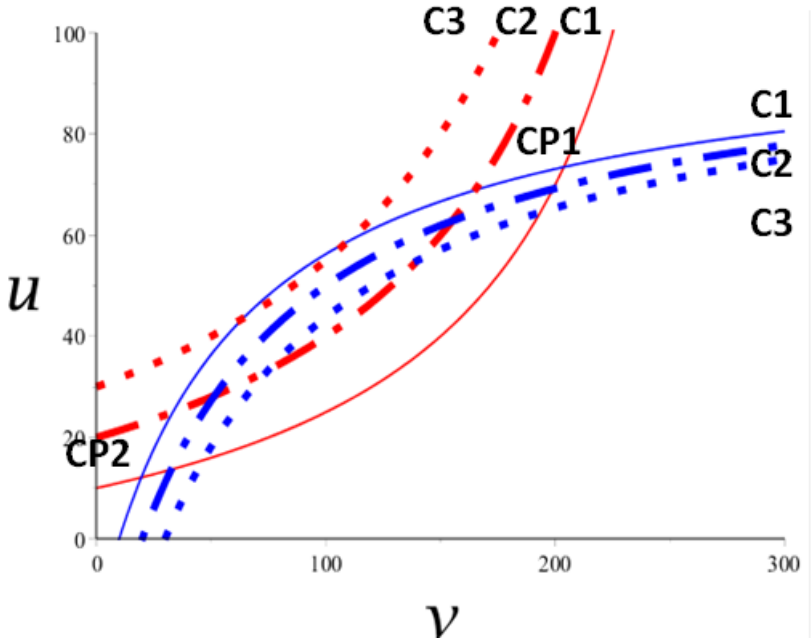


Figure 3. Nullclines for Cases 1, 2, and 3

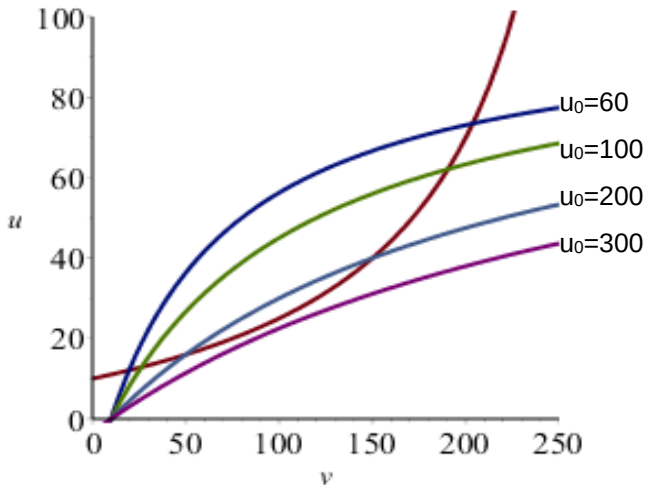


Figure 4. Impact of Changes to u_0 in Case 1

I now focus on the impact of operational changes on a system. In particular, I am interested in those parameters that changes in the level of security (S) and in investment (I) in the system will likely influence. I take security to be anything (capital, procedure, etc.) that reduces attacks or their severity. Similarly, investment includes any other activity (other than use) that increases the system's capability or capacity. I conduct the analysis in two parts. First, I infer the impact on the parameters from changes in security and investment. Then, I consider the impact on the critical point of changes in the various parameters in a numerical example. In particular, I focus on the movement of the positive coexistence critical point (i.e., the one farthest from the origin).

One can estimate the impact of changes in security by evaluating first derivative of V* (the value of V at the coexistence critical point) with respect to S and with respect to I as Equations 11 and 12 shows.

$$\frac{\partial V^*}{\partial s} = \frac{\partial V^*}{\partial v_1}\frac{\partial v_1}{\partial s} + \frac{\partial V^*}{\partial v_2}\frac{\partial v_2}{\partial s} + \frac{\partial V^*}{\partial u_1}\frac{\partial u_1}{\partial s} + \frac{\partial V^*}{\partial u_2}\frac{\partial u_2}{\partial s} \quad (11)$$

$$\frac{\partial V^*}{\partial I} = \frac{\partial V^*}{\partial K_u}\frac{\partial K_u}{\partial I} + \frac{\partial V^*}{\partial K_v}\frac{\partial K_v}{\partial I} \quad (12)$$

First, I consider the impact of investment or security changes. Substantial research demonstrates that computer security imposes costs on users (Lampson, 2009). In a study of how people experience security, Dourish, Grinter, Delgado de la Flor, and Joseph (2004) found that users cared about security but were neutral to negative in their attitudes toward it. Post and Kagan (2007) reported that security interfered with user tasks for many users.

It seems likely that increases in security will result in increases both in v_1 and u_1 since increases in security will likely reduce usability and, thus, increase "death rates" of users and value. It also seems likely that increases in security will decrease v_2 and u_2 since the cost of security will decrease the value of the interaction. In the two-population case, there are no attackers, so security is a pure cost. Further, it seems likely that increased investment will increase both K_u and K_v since it will increase capacity (K_u) and capability (K_v). Table 5 summarizes these inferences in the "inferred" column. I calculated the partials of V* with respect to its parameters at the stable critical point for Case 1 (203,73) (see "calculated" column in Table 5 and section 6 in Appendix B).

Table 5. Impact of Changes in Security (S) and Investment (I)

Inferred	Calculated
$\frac{\partial v_1}{\partial s} \geq 0$	$\frac{\partial V^*}{\partial v_1} = -358 \leq 0$
$\frac{\partial v_2}{\partial s} \leq 0$	$\frac{\partial V^*}{\partial v_2} = 3581 \geq 0$
$\frac{\partial u_1}{\partial s} \geq 0$	$\frac{\partial V^*}{\partial u_1} = -43 \leq 0$
$\frac{\partial u_2}{\partial s} \leq 0$	$\frac{\partial V^*}{\partial u_2} = 436 \geq 0$
$\frac{\partial K_v}{\partial I} \geq 0$	$\frac{\partial V^*}{\partial K_v} = .76 \geq 0$
$\frac{\partial K_u}{\partial I} \geq 0$	$\frac{\partial V^*}{\partial K_u} = .84 \geq 0$

I evaluate the signs of the terms on the right hand side of Equations 11 and 12 using the signs in Table 5. The terms in each of the first four rows have opposite signs, so, when one considers the signs of the terms on the right hand sider of Equation 11, in Equation 11, one gets:

$$\frac{\partial V^*}{\partial s} \leq 0 \quad (13)$$

Similarly, terms in the last two rows in Table 5 have the same sign, so that Equation 12 reveals:

$$\frac{\partial V^*}{\partial I} \geq 0 \quad (14)$$

The consequence of Equations 13 and 14 is that increased security results in decreased system value and that increased investment results in increased system value. Both of these results are as one would expect in a world with no attackers.

4 Three-population Model

In this section, I extend the two-population model to include a population of attackers that act as predators of the IS; here, the IS itself serves as a host species for the attackers. The user remains in a mutualistic relationship with the system value. I make three additional assumptions:

- When the attacker population is small, the system looks like the two-population model.
- The system value changes decreases with attacks.
- The rate of attacks increases with system value.
- The impact of attack on value is proportional to the product of system value and attacker population

I acknowledge that these are strong assumptions and that data are not readily available to confirm them empirically. Put another way, the model says that the rate of change in value, as a fraction of current value, is proportional to the number of attacks. Similarly, the rate of change in the number of attacks as a fraction of total attacks is proportional to the system's value. These assumptions are consistent with the assumptions of a predator-prey ecology (Smith, 1974).

The last of the new assumptions merits some discussion. In basic predator-prey models such as the Lotka-Volterra model (Brauer & Castillo-Chavez, 2001), the birth rate of predators is assumed to be proportional to the product of the predator population and the prey population: $\frac{d\,N_{pred.}}{dt} = -k\,N_{prey}\,N_{pred} + birth\,rate_{Pred} * N_{pred}$. The first factor in the first term relates to the number of predators available for breeding. The second factor relates to food supplies. The more prey there are, the more likely predators are to encounter them (density of predators * density of prey), and so the more births will occur to increase the predator population. A similar term with opposite sign occurs in the equation for prey. Max Vision, a major cyber-criminal, conducted systematic scans of IP addresses for ports with known weaknesses (Poulsen, 2011). His approach seems similar to the search of predator for prey. There are many other examples of a product term's being used to model interaction between species. Xiang, Zhou, and Li (2006) propose an attack defense model of distributed denial-of-service attacks (DDOS) based on the Lanchester warfare model (Lanchester, 1956; Davis, 1995). Similar relationships occur in epidemiology (Brauer & Castillo-Chavez, 2001), chemical kinetics (Amdur & Hammes, 1966; Strogatz, 1994), economics (Goodwin, 1982; Sportelli, 1994; Dendrinos & Mullally, 1981).

Absent specific consideration of difficulty or punishment (which the current model does not include), it seems reasonable to assume that the supply of attacks will vary with the value of the targets and vice versa. Verizon (2014, p. 9) notes that "money-motivated breaches still outnumber others by a good margin", and Symantec (2015) notes that spear phishing attacks (a targeted email phishing attack) have risen greatly, which suggests that criminals have become more selective about their choice of targets. Both sources suggest that high target value motivates attacks.

The model is also consistent with foraging theory's notion of information as value (Pirolli & Card, 1995). Verizon (2015, p. 5) notes that, "in 70% of the attacks where we know the motive, there's a secondary victim". So, as an example, subverting a website to infect visitors illustrates the principle: if the number of visitors to a website increases (i.e., its value increases), then its attraction to attackers will also increase. This area is clearly one where empirical research would be useful (e.g., by validating these assumptions and estimating parameters).

4.1 The Model

$$\dot{V} = -v_1 V + v_2 UV\left(1 - \mathrm{V}\frac{v_0 + U}{K_v U}\right) - v_3 \mathrm{AV} \tag{15}$$

$$\dot{U} = -u_1 U + u_2 UV\left(1 - \mathrm{U}\frac{u_0 + V}{K_u V}\right) \tag{16}$$

$$\dot{A} = -a_1 A + a_2 AV \tag{17}$$

In these equations, V = the value of the system, U = the population of users (proxy for the amount of use), A = the volume of attacks, and all of the parameters are assumed positive.

Equations 15 and 16 reflect the mutualism between user and system. Equations 15 and 17 reflect the predator-prey relationship between the attackers and the system. The parameters are similar to the two-population model with additional parameters for attackers and for the attacker value interaction. The parameter a_1 is the rate of attrition for attackers perhaps due to death or retirement. Similarly, a_2 is its "growth" rate. Since A and V do not have a mutualistic relationship, no one does not need an upper bound on A.

4.2 Solution

To evaluate such a system of equations, I again identify the nullclines and critical points. To determine the nullclines, I set $\dot{V}, \dot{U},$ and $\dot{A}$ equal to 0. One can immediately note that V = 0, U = 0, and A = 0 are nullclines and that there is a critical point at the origin. I then factor out V, U, and A from Equations 15, 16, and 17, respectively, and get the following:

$$-\mathrm{v}_1 + \mathrm{v}_2\left(\mathrm{U} - \mathrm{V}\frac{\mathrm{v}_0 + \mathrm{U}}{K_\mathrm{v}}\right) - \mathrm{v}_3\mathrm{A} = 0 \tag{18}$$

$$-\mathrm{u}_1 + \mathrm{u}_2\left(\mathrm{V} - \mathrm{U}\frac{\mathrm{u}_0 + \mathrm{V}}{\mathrm{K}_\mathrm{u}}\right) = 0 \tag{19}$$

$$-\mathrm{a}_1 + \mathrm{a}_2\mathrm{V} = 0 \tag{20}$$

One can arrange Equations 18, 19, and 20 to give:

$$\mathrm{UV} + \mathrm{v}_0\mathrm{V} - \mathrm{K}_\mathrm{v}\mathrm{U} + \frac{\mathrm{v}_3}{\mathrm{v}_2}\,\mathrm{K}_\mathrm{v}\mathrm{A} + \frac{\mathrm{v}_1}{\mathrm{v}_2}\,\mathrm{K}_\mathrm{v} = 0 \tag{21}$$

$$\mathrm{UV} + \mathrm{u}_0\mathrm{U} - \mathrm{K}_\mathrm{u}\mathrm{V} + \frac{\mathrm{u}_1}{\mathrm{u}_2}\,\mathrm{K}_\mathrm{u} = 0 \tag{22}$$

$$\mathrm{V} - \frac{\mathrm{a}_1}{\mathrm{a}_2} = 0 \tag{23}$$

Solving Equations 21, 22, and 23 gives:

$$A^* = \frac{UVv_2 + v_0v_2V - K_vv_2V + K_vv_1}{K_vv_3} \tag{24}$$

$$U^* = \frac{K_u\,(Vu_2 - u_1)}{u_2(u_0 + V)} \tag{25}$$

$$V^* = \frac{a_1}{a_2} \tag{26}$$

Equations 24 and 25 describe hyperbolic surfaces. Table 6 provides the asymptotes and intercepts. Figure 5 shows the general appearance of these curves for the parameters of Case 4, which Table 7 lists. Figure 6 illustrates the region in the vicinity of the non-zero critical point. Equation 27 shows the Jacobian for this system (see section 7 in Appendix B).

Table 7 shows the solution. Since it is in the positive octant, it is economically feasible. Since all three of the eigenvalues are real and negative, it follows that the critical point is stable. Since it is in the positive octant, it is economically feasible.

Table 6. Three-population Asymptotes and Intercepts

	Asymptotes		Intercepts	
	$V \to \infty$	$U \to \infty$	$V = 0$	$U = 0$
V null cline (14a)	$U = -v_0$	$V = K_v$	$U = (v_1+Av_3)/v_2$	$V = -(v_1K_v+Av_3K_v)/v_0v_2$
U null cline (14b)	$U = K_u$	$V = -u_0$	$U = -k_uu_1/u_0u_2$	$V = u_1/u_2$

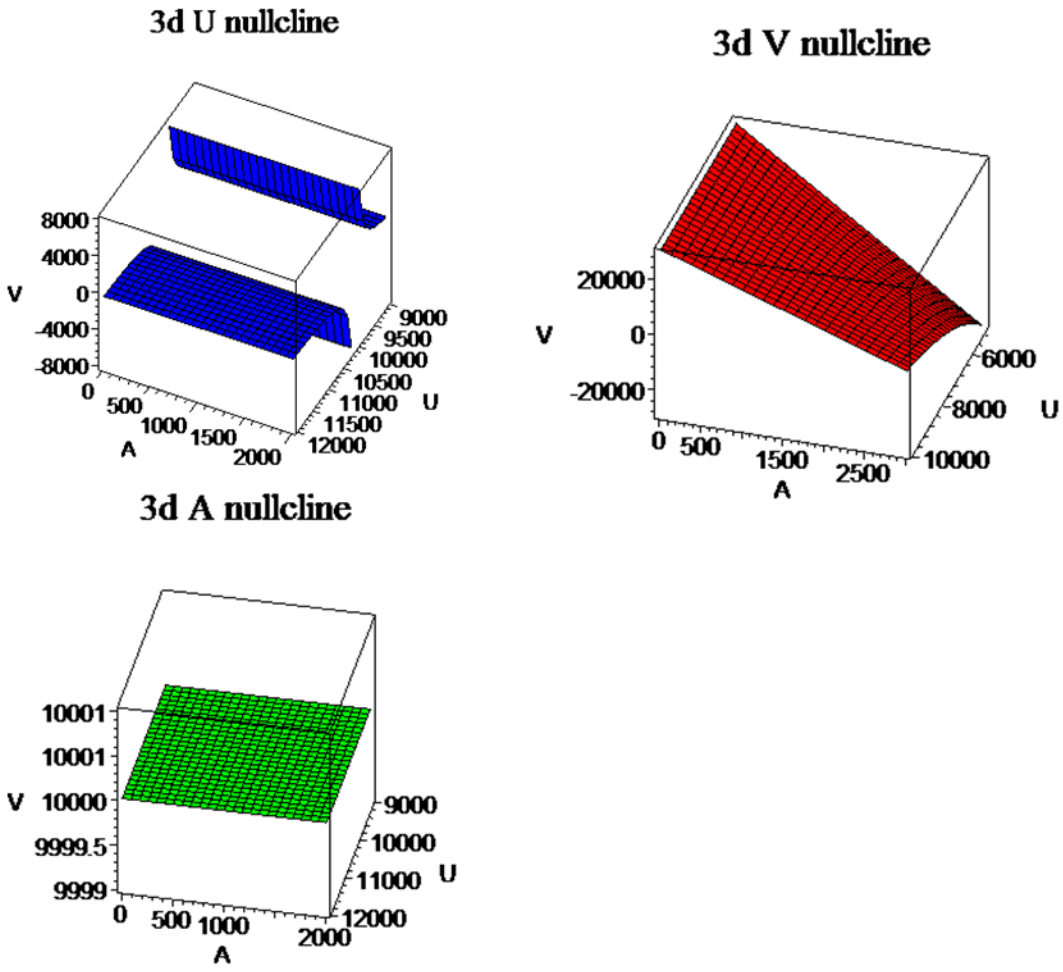


Figure 5. Nullclines for Three Species

Table 7. Behavior at the Critical Point for Various Parameters

Parameters	Case 4	Case 5	Case 6
K_v	30000	30000	30000
K_u	10000	10000	10000
v_0	100	100	100
v_1	0.001	0.001	0.001
v_2	0.03	0.03	0.03
v_3	0.1	0.1	0.1
u_0	100	100	100
u_1	0.01	0.01	0.01
u_2	0.01	0.01	0.01
a_1	0.1	0.1	0.1
a_2	0.00001	0.00006	0.001
Calculated resultant values			
V*	10000	1667	100
U*	9900	9428	4950
A*	1969	2670	1479
Eigenvalues	-114	-31.8	-8.60
	-85.8	-0.356-3.72 I	0.248
	-0.201	-0.356+3.72 I	6.86
Character	stable	stable spiral	unstable

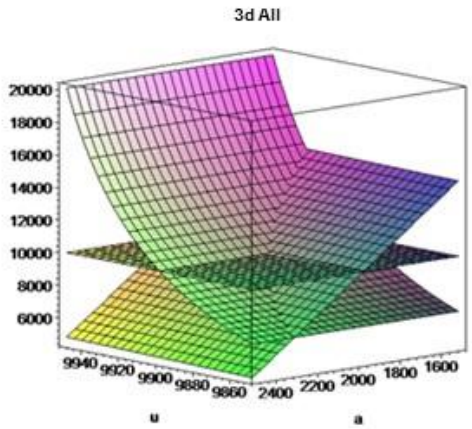


Figure 6. Vicinity of the Non-zero Critical Point (Case 4)

$$J = \begin{bmatrix} -100 & 200 & -1000 \\ 0.99 & -100 & 0 \\ 0.197 & 0 & 0 \end{bmatrix} \tag{27}$$

4.3 Critical Point Evaluation

One can calculate the values of the critical points from Equations 24, 25, and 26. The general procedure for characterizing the critical points is as follows: one calculates the eigenvalues of the Jacobian. In general, eigenvalues may be complex numbers. If any of the real parts is positive, the point is not stable.

Negative real parts indicate stable points. One evaluates the eigenvalues by looking at the imaginary part. If the eigenvalues are all real, the point is a sink. If complex, then the point is a spiral.

It is difficult to solve problems of this complexity using analytical methods. In particular, finding the eigenvalues of the Jacobian in closed form is very hard. As such, I considered and evaluated several cases numerically. As in the two-dimensional case, I chose parameters to illustrate the range of possible behaviors. In choosing those cases, I made some effort to make the relationships between the parameters plausible at least in order of magnitude. As Table 7 shows (see also section 8 in Appendix B), there are sets of parameters that realize stable, spiral, and unstable systems.

The three cases in Table 7 have the same parameter values except for a_2, the rate at which attacks benefit attackers. As the value of a_2 changes, the system experiences phase changes. When a_2 is small, the system is stable; as a_2 increases, the system evolves to a stable spiral and, finally, to an unstable system. I chose a_2 for this analysis since it seems to be a way to characterize different types of attackers. Small values of a_2 would model less serious attackers, while larger values of a_2 would model serious criminals who are attracted by high value targets, so these responses seem consistent with expectations. In a similar fashion, one might expect a low value of a_1 with state-sponsored attackers who have a low attrition rate due to the state support. Performing similar sensitivity analysis for the other parameters still needs to be done. In particular, it would be interesting to do a joint sensitivity analysis with a_2 and v_3 (the sensitivity of the system to attack).

Figures 7 and 8 show three-dimensional evolutions in the state space for cases 4 and 5. I created the trajectories with ODEToolkit (Harvey Mudd College, 2013). The axes are U, V, and A. One can easily see that the systems are, indeed, stable. Figure 8 illustrates the spiral of Case 5. In Figures 7 and 8, the o symbol represents initial conditions, and the x symbol represents ending states (see Appendix D for setup).

We have already seen that social media sites can fail due to lack of use and value and that cyberattacks may cause severe loss of value (Ponemon Institute, 2012) and possibly business failure. Recently, Altegrity, citing a cyberattack, filed for bankruptcy (Brickley, 2015). In testimony before the Subcommittee on Small Business of the U.S. House of Representatives, Shapero (2013) suggested that most small businesses could not survive a cyberattack that involved a data breach.

Note that the stable spiral suggests a situation in which there are waves of attacks to which defenders respond, which results in oscillating value as the system approaches equilibrium. Data are not readily available to illustrate this sort of behavior, but one can easily conceive it.

To clarify the spiral case, I plotted V against time (Figure 9). As one can see, V appears to have a damped oscillation. Other authors have found similar fluctuations in security and financial systems. Rosenfeld et al. (2007) present a dynamic model of computer security that combines limits to growth with escalation prototypes. Under some circumstances, their model exhibits oscillating behavior. Muchnik and Solomon (2003) simulate financial markets as systems of three types of interacting agents. Their results also predict damped oscillations under certain circumstances. Such oscillations may be due partly to delays in feedback loops as seen in the beer game (Senge, 1990; Sterman, 1989).

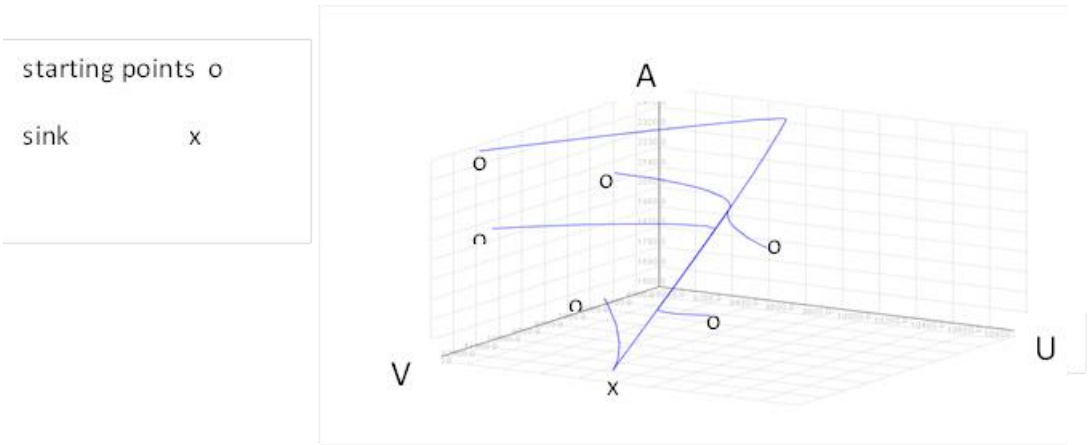


Figure 7. State Space Evolution of Case 4

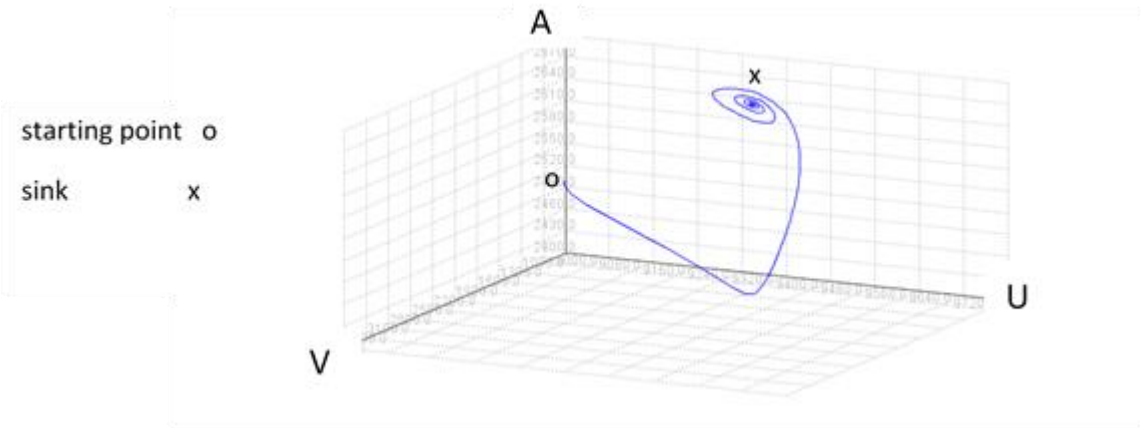


Figure 8. State Space Evolution of Case 5

Figure 9. Value Versus Time for Case 5

4.4 Sensitivity Analysis

I begin the sensitivity analysis by extending the marginal analysis of the two-population model. In the three-population model, $\frac{\partial V^*}{\partial s}$ has three additional terms as Equation 28 shows:

$$\frac{\partial V^*}{\partial s} = \frac{\partial V^*}{\partial v_1}\frac{\partial v_1}{\partial s} + \frac{\partial V^*}{\partial v_2}\frac{\partial v_2}{\partial s} + \frac{\partial V^*}{\partial u_1}\frac{\partial u_1}{\partial s} + \frac{\partial V^*}{\partial u_2}\frac{\partial u_2}{\partial s} + \frac{\partial V^*}{\partial a_1}\frac{\partial a_1}{\partial s} + \frac{\partial V^*}{\partial a_2}\frac{\partial a_2}{\partial s} + \frac{\partial V^*}{\partial v_3} \quad (28)$$

The sort of analysis used previously reveals that the three new terms are all positive in sign as expected. Pendegraft and Rounds (2007) notes that their simulation model had states in which increasing security caused the value of the system to decrease. Thus, one can ask under what circumstances will increasing security cause the value of the system to increase. In other words, when is $\frac{\partial V^*}{\partial s} > 0$? Rearranging Equation 28 gives the condition for $\frac{\partial V^*}{\partial s} > 0$:

$$\frac{\partial V^*}{\partial a_1}\frac{\partial a_1}{\partial s} + \frac{\partial V^*}{\partial a_2}\frac{\partial a_2}{\partial s} + \frac{\partial V^*}{\partial v_3}\frac{\partial v_3}{\partial s} > -\left(\frac{\partial V^*}{\partial v_1}\frac{\partial v_1}{\partial s} + \frac{\partial V^*}{\partial v_2}\frac{\partial v_2}{\partial s} + \frac{\partial V^*}{\partial u_1}\frac{\partial u_1}{\partial s} + \frac{\partial V^*}{\partial u_2}\frac{\partial u_2}{\partial s}\right) \quad (29)$$

Note that the model does not assume that a particular security technology affects only one parameter. On the contrary, I suspect that most security measures affect more than one. For example, increased perimeter protection (longer passwords, firewalls, etc.) may cause increases in a_1 and decreases in a_2. Clearly, we need empirical work to estimate the various factors in particular situations. Rounds, Pendegraft, and Alves Foss (2013) report on efforts to experimentally evaluate such parameters for a related simulation model.

Since one can analytically evaluate the critical point, I conducted a limited marginal analysis on V*. That is, I examined the impact on V* of changes in the parameters. There are presumably three ways to improve a system's value with security: by reducing the number of attackers (via a_1), by reducing the impact of an attack on V (via v_3), and by reducing the benefit to the attackers (via a_2). All three methods reduce the attackers' numbers. Since V* = a1/a2, one can calculate the impact of changes in various parameters. In particular, I note that:

$$\frac{\partial V^*}{\partial a_1} = \frac{1}{a_2} > 0 \tag{30}$$

$$\frac{\partial V^*}{\partial a_2} = -\frac{a_1}{a_2^2} < 0 \tag{31}$$

And that:

$$\frac{\partial V^*}{\partial v_3} = 0. \tag{32}$$

The signs of the derivatives in 30 and 31 seem as expected. Increasing a_1 (death rate of attackers) should increase the value of the system. Likewise, decreasing a_2, the rate at which attackers benefit from attacks, should also increase V*. However, the third result is surprising. It suggests that changing the impact of attacks on the system results in no change in the critical point, nor does changing any other parameter change the value of V*. The policy implication is clear: for stable solutions, it is better to reduce the number of attackers or to reduce their rewards from attacking than to reduce their impact on the system. In other words, a policy that reduces number of attackers or the benefits that they derive is better than a damage-control policy. In particular, reducing the number of attackers is attractive.

It is interesting to consider whether these results offer useful implications for individual firms or governments. The current model has only a single target, so it does not illuminate issues associated with attacker choice (see Sandler and Lapan (1988) for a discussion of attacker choice in terrorism). Most individual firms can suitably harden their systems to reduce the rewards to attackers and, thus, perhaps reduce the number of attacks on their own systems, but they can probably not reduce the total number of attackers. However, Microsoft's recent efforts to assist in the law-enforcement effort to bring down a fraud botnet suggests that an individual firm with significant technical and economic resources can directly reduce the number of attackers (Stewart & Marr, 2013). Indeed, there may be a business opportunity here for a firm with adequate resources to directly go after attackers via legal or technical means. This event also illustrates the importance of law enforcement and diplomatic efforts to reduce the number of attackers.

The current state of law and technology makes such a policy difficult (Davenport, 2002). The results suggest that legal remedies could be of value if one can identify attackers and reach them through the legal system. Such measures require knowing the identity of the attackers, and, as Armstrong and Forde (2003) note, anonymity on the Internet is a serious security issue. The three-population model supports their concern. Given this difficulty, the three-population model recommends keeping attackers out rather than controlling damage. Indeed, it suggests that damage control has little value.

Now, substitute the results (30, 31, 32) into Equation 29 and note that all of the terms on the right hand side of Equation 29 are 0 since they contain derivatives of V* with respect to variables on which it does not depend.

$$\frac{\partial V^*}{\partial a_1}\frac{\partial a_1}{\partial s} + \frac{\partial V^*}{\partial a_2}\frac{\partial a_2}{\partial s} > 0 \quad (33)$$

Substituting 30 and 31 into 33 gives:

$$\frac{1}{a_2}\frac{\partial a_1}{\partial s} - \frac{a_1}{a_2^2}\frac{\partial a_2}{\partial s} > 0 \quad (34)$$

Which gives:

$$\frac{\partial a_1}{\partial s} > V^* \frac{\partial a_2}{\partial s} \quad (35)$$

The inequality in Equation 35 is a condition for increased security's being desirable in the sense of increasing V. It seems likely that $\frac{\partial a_1}{\partial s} > 0$ (increased death rate) and that $\frac{\partial a_2}{\partial s} < 0$ (decreased growth rate). Hence, this result (Equation 35) would seem to hold in most cases. Since the simulation results I refer to earlier (Pendegraft & Rounds, 2007) suggest otherwise, my results suggest that the current model does not adequately consider the direct costs of security on the system. It remains to extend the model in this way.

One might ask under what conditions:

$$\frac{\partial V^*}{\partial a_1} > -\frac{\partial V^*}{\partial a_2} \quad (36)$$

That is, when is it better to increase the death rate of attackers rather than reduce the benefit they receive? Reducing the benefit means decreasing a_2, which explains the negative sign on the right hand side of Equation 35. That condition is met when:

$$a_2 > a_1 \quad (37)$$

That is, it is better to reduce the benefits of attacking (i.e., harden the site) when the marginal impact of that action on the attackers is greater than the current attacker "death rate".

5 Discussion

While I made no effort to assign empirically determined values to the parameters, I did try to keep the relative magnitudes of the parameters reasonable. For example, death rates are all of magnitude 0.1, which seems plausible. However, since I do not specify the basic units of the variables (V,U, and A), I made no more accurate attempt to estimate the parameters, which presents an opportunity for future work. Rounds et al. (2013) report on efforts to experimentally evaluate such parameters for a related simulation model.

The general result of the model is consistent with what one would expect from a real system. Consider the two population cases illustrated with numeric examples. In the first, the two nullclines intersect in the real plane, which gives one coexistence critical point, a stable equilibrium at the origin, and a saddle point between them. Thus, there is a set of points "close" to the origin that will evolve to the origin (i.e., extinction of the system). Initial conditions "farther" from the origin will evolve to the stable equilibrium point, which is consistent with the notion that sufficient resources must be invested in an information system to "jump start" it. That is, it is necessary to provide sufficient investment to provide enough value to initial users to allow the system to survive.

In Case 3 of the two-population model and Case 6 of the three-population model, the nullclines do not intersect at all. In these cases, the only stable point is the origin, which means that the system will run to extinction of both value and users. Thus, it is important from a design point of view to be able to

distinguish between these two types of situations and, in the first (with intersecting nullclines), to ensure that sufficient capital is deployed initially to give initial conditions of V in the viable area. The sensitivity analysis suggests that increases in security may move the coexistence equilibrium closer to the origin and, thus, reduce the system's value.

There are several interesting policy implications from the three-population model: 1) that active measures against attackers by law enforcement or diplomatic efforts have value and 2) that hardening a target in such a way as to deny value to attackers also has merit. Defensive measures taken to preserve value, on the other hand, do not. The results call into question the merits of storing customer credit card numbers. Stored numbers, if compromised, can create value for attackers (by increasing a_2), while the additional value created by their storage (increased v_2) does not affect the critical point.

The fact that some security measures such as backups seem to have no impact on V* is interesting. At least two reasons can explain this result. First, the model does not reflect destruction of system components by attack but rather the reduction in their value. Second, the model does not consider natural disasters that do commonly destroy systems. Thus, backup and restoration have no impact on V* in the model. Since natural disasters are relatively rare, modeling them as random phenomena that temporarily increase v_1 (i.e. treating v_1 as an random variable) seems reasonable. Doing so is beyond the scope of this paper, but it could be a profitable extension to this model (I thank an anonymous reviewer for drawing my attention to this matter).

The model presented here demonstrates that it is possible for a system to be stable and that its behavior closely depends on its parameters. The model has several limitations. The first is that it is inherently simple. The second is that it is static in the sense that the parameters are constant over time. The third is that it does not consider the direct costs of security measures. The fourth is that it does not consider other modes of system failure. Future work can perhaps address these limitations. As I note throughout the paper, opportunities abound for conducting further sensitivity analyses on the model.

One major open issue has to do with attacker choice. If different targets have different parameter values, how will attackers choose how to allocate their efforts between targets? This issue is especially important in light of the notion that hardening a website is a good defensive strategy. Likewise, not all attackers are identical: how should defenders react in a world with different sorts of attackers?

Clearly, we need much empirical work needs before one can use this model to develop policies for specific systems. In particular, one would need to empirically evaluate specific macro-economic parameters. This need highlights a major problem in current thinking about information security; namely, that we do not adequately understand the character and motivation of attackers. Indeed, we do not adequately understand the economics of using information systems. I hope that this work will be a small step in improving that understanding.

Acknowledgments

I thank the anonymous reviewers for their many very helpful comments. I am especially indebted to the senior editor for an unusually thorough and helpful review including many helpful suggestions.

References

Addicott, J. F., & Freedman, H. I. (1984). On the structure and stability of mutualistic systems: Analysis of predator-prey and competition models as modified by the action of a slow growing mutualist. *Theoretical Population Biology*, *26*(3), 320-229.

Addicott, J. F. (1981). Stability properties of a 2-species models of mutualism: Simulation studies. *Oceologiia*, *49*(1), 42-49.

Amdur, I., & Hammes, G. (1966). *Chemical kinetics: Principles and selected topics.* New York: McGraw Hill.

Anderson, R., & Moore, T. (2007). Information security economics—and beyond. In *Proceedings of the International Cryptology Conference* (pp. 68-91).

Armstrong, H. L., & Forde, P. J. (2003). Internet anonymity practices in computer crime. *Information Management and Computer Security*, *11*(5), 209-215.

Becker, G. S. (1968). Crime and punishment: An economic approach. Journal of Political Economy 78, 169-217.

Behara, R. R., Huang, C. D., & Hu. Q. (2010). A systems dynamics model of information security investments. Journal of Information System Security, 6(2), 30-44.

Betz, D., & Stevens, T. (2013). Analogical reasoning and cyber security. *Security Dialog, 44*(2), 147-162.

Bishop, M. (2003). *Computer security: Art and science*. Boston, MA: Addison Wesley.

Boyce, W. E., & Diprima, P. C. (2005). *Elementary differential equations* (8th ed.). Hobokan: Wiley.

Brauer, F., & Castillo-Chavez, C. (2000). *Mathematical models in population biology and epidemiology*. New York: Springer-Verlag.

Braun W. (2002). *The system archetypes.* Retrieved from http://www.albany.edu/faculty/gpr/PAD724/724WebArticles/sys_archetypes.pdf

Brickley, P., (2015). Altegrity gets final OK on bankruptcy finance, lender pact. *The Wall Street Journal*. Retrieved from http://www.wsj.com/articles/altegrity-gets-final-ok-on-bankruptcy-finance-lender-pact-1426536470

Bronstein, J. (1994). Our current understanding of mutualism. *Quarterly Review of Biology*, *69*(1), 31-51.

Chau, P. Y. K., & Hui, K. L. (1998). Identifying early adopters of new IT products: A case of Windows. *Information & Management, 33*(5), 225-230.

Chmielewski, D. C., & Sarno, D. (2009). How MySpace fell off the pace. *The Los Angeles Times*. Retrieved from http://articles.latimes.com/2009/jun/17/business/fi-ct-myspace17

Crandall, J. R., Ensafi, R., Forrest, S., Ladau, J., & Shebaro, B., (2008). The ecology of malware. In *Proceedings of the New Security Paradigms Workshop* (pp. 99-106).

Davenport D., (2002). Viewpoint: Anonymity on the Internet: Why the price may be too high. *Communications of the ACM*, *45*(4), 33-35.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, *13*(3), 319-340.

Davis, P. K. (1995). *Aggregation, disaggregation, and the 3:1 rules in ground combat.* Santa Monica, CA: RAND Corporation.

Dean, A. M. (1983). A simple model of mutualism. *American Naturalist, 121*, 409-417.

DeLone, W. H., & McLean, E. R., (1992). Information system success: The quest for the dependent variable. *Information Systems Research*, *3*(1), 60-95.

Dendrinos, D., & Mullally, H. (1981). Evolutionary patterns of urban populations. Geographical Analysis 13, 328-344.

Digital Trends Staff. (2014). The history of social networking. *Digital Tends*. http://www.digitaltrends.com/features/the-history-of-social-networking/

Dourish, P., Grinter, R., Delgado de la Flor, J., & Joseph, M. (2004). Security in the wild: User strategies for managing security as an everyday, practical problem. *Personal and Ubiquitous Computing*, *8*(6), 391-401.

Dutta, A., & Roy, R. (2008). Dynamics of organizational information security. *System Dynamics Review*, *24*(3), 349-375.

Ernst & Young. (2012). 2012 global information security survey: Fighting to close the gap. Retrieved from http://www.ey.com/gl/en/services/advisory/2012-giss---fighting-to-close-the-gap---overview

Freedman, H. I., Addicott, J. F., & Rai, B. (1987). Obligate mutualism with a predator: Stability and persistence of three species models. *Theoretical Population Biology, 32*, 157-175.

Furnell, S. (2008). It's a jungle out there: Predators, prey and protection in the online wilderness. *Computer Fraud & Security*, *10*, 3-6.

Garcia, D., Mavrodiev, P., & Schweitzer, F. (2013). Social resilience in online communities: The autopsy of friendster. In *Proceedings of the ACM Conference on Social Networks*.

Goodwin, R. M. (1982). A growth cycle. In R. M. Goodwin (Ed.), *Essays in economic dynamics* (pp. 165-170). London: Macmillan.

Gordon, L. A., & Loeb. M. P. (2002). The economics of information investment. *ACM Transactions on Information and System Security*, *5*(4), 438-457.

Hannan, M., & Freeman J. (1977). The population ecology of organizations. *American Journal of Sociology*, *82*(5), 929-964.

Harvey Mudd College. (2013). *ODEToolkit*. Retrieved from http://odetoolkit.hmc.edu/

Herzog, A., Shahmehri, N., & Duma, C. (2007). An ontology of information security. *International Journal of Information Security and Privacy*, *1*(4), 1-23.

Hoeksema, J. D., & Schwartz, M.W. (2003). Expanding comparative-advantage biological market models: Contingency of mutualism on partners' resource requirement and acquisition trade-offs. *Proceedings of the Royal Society of London*, *270*(1518), 913-919. Internet Crime Complaint Center. (2013). *2012 Internet crime report*. Retrieved from http://www.ic3.gov/media/annualreport/2012_IC3Report.pdf

Jorgensen, J., Rossignol, P., Takikawa, M., & Upper, D. (2001). Cyber ecology: Looking to ecology for insight into information assurance. In *Proceedings of the DARPA Information Survivability Conference & Exposition II* (pp. 287-296).

Lampson, B. (2009). Privacy and security: Usable security: How to get it. *Communications of the ACM, 52*(11), 25-27.

Lanchester F. W. (1956). Mathematics in warfare. In J. R. Newman (Ed.), *The world of mathematics* (vol. 4, pp. 2138-2157). New York: Simon and Schuster.

McGill, B. (2005). A mechanistic model of a mutualism and its ecological and evolutionary dynamics. *Ecological Modeling*, *187*, 413-425.

Mehlun, H., Moene, K., & Torvik, R. (2003). Predator or prey? Parasitic enterprises in economic development. *European Economic Review*, *47*, 275-294.

Mishra, B. K., & Jha, N. (2010). SEIQRS model for the transmission of malicious object sin computer network. *Applied Mathematical Modeling*, *34*, 710-715.

Mishra, B. K., & Saini, D. K. (2007). SEIRS epidemic model with delay for transmission of malicious objects in computer network. *Applied Mathematics and Computation*, *188*, 1476-1482.

Muchnik, L., & Soloman, S. (2003). Statistical mecahanics of conventional traders may lead to non-conventional market behavior. *Phsica Scripta*, *T106*, 41-47.

Novakovic, L., McGill, T., & Dixon, M. (2009). Understanding user behavior towards passwords through acceptance and use modeling. *International Journal of Information Security and Privacy, 3*(1), 11-29.

Pendegraft, N., & Rounds, M. (2007). Simulation model of information systems security. *International Journal of Information Security and Privacy, 1*(4), 62-74.

Pirolli, P., & Card, S. (1995). Information foraging in information access environments. In *Proceedings of ACM Conference on Human Factors in Computing Systems.* Retrieved from http://www2.parc.com/istl/groups/uir/publications/items/UIR-1995-07-Pirolli-CHI95-Foraging.pdf

Pirolli, P. (2009). An elementary social information foraging model. In *Proceedings of the Conference on Computer-Human Interaction.*

Ponemon Institute. (2012). *2012 cost of cyber crime study: United States*. Retrieved from http://www.ponemon.org/local/upload/file/2012_US_Cost_of_Cyber_Crime_Study_FINAL6%20.pdf

Post, G., & Kagan, A. (2007). Evaluating information security tradeoffs: Restricting access can interfere with user tasks. *Computers & Security*, *26*(3), 229–237.

Poulsen, K. (2011). *Kingpin: How one hacker took over the billion-dollar cybercrime underground*. New York: Crown Publishers.

Rai, B., Freedman, H. I., & Addicott, J. F. (1983). Analysis of three species models of mutualism in predator-prey and competitive systems. *Mathematical Biosciences*, *65*, 13-50.

Rosenfeld, S., Rus, I., & Cukier, M. (2007). Archetypal behavior in computer security. *Journal of Systems and Software*, *80*(10), 1594-1606.

Rounds, M., Pendegraft, N., & Taylor, C. (2007). *The ecology of IS security: A research agenda*. Paper presented at the Information Resources Management Association International Meeting.

Rounds, M., Pendegraft, N., & Alves Foss, J., (2013). An experimental study to explore attacker response to changes in security and reward. In *Proceedings of the 46th Hawaii International Conference On System Sciences.*

Saltzer, J. H., & Schroeder, M. D. (1975). The protection of information in computer systems. *Proceedings of the IEEE*, *63*(9), 1278-1308.

Sandler, T., & Lapan, H. (1988). The calculus of dissent: An analysis of terrorist choice of targets. Synthese, *76*(2), 245-261.

Senge, P. (1990). *The fifth discipline*. New York: Doubleday.

Shapero, D. (2013). Protecting small businesses against emerging and complex cyber-attacks (hearing). *Small Business Committee.* Retrieved from http://smallbusiness.house.gov/calendar/eventsingle.aspx?EventID=323427

Smith, M. (1974). *Models in ecology*. Cambridge: Cambridge University Press.

Sportelli, M. (1994). A Kolmogoroff generalized predator prey model of Goodwin's growth cycle. *Journal of Economics*, *61*(1), 35-64.

Sproles, G. B. (1974). Fashion theory: A conceptual framework. *Advances in Consumer Research*, *1*, 463-472.

Sterman, J. D. (1989). Modeling managerial behavior: misperceptions of feedback in a dynamic decision making experiment. *Management Science, 35*(3), 321-339.

Sterman, J. D. (2000). *Business dynamics*. Boston: McGraw Hill.

Stewart, C., & Marr, M. (2013). Inside the effort to kill a Web fraud "botnet". *The Wall Street Journal*. Retrieved from http://online.wsj.com/news/articles/SB10001424052702303722104579240151385337672?KEYWORDS=microsoft

Strogatz, S. (1994). *Nonlinear dynamics and chaos*. Cambridge: Perseus.

Symantec. (2015). *Internet security threat report*.

Thrimbleby, H., Anderson, S., & Cairns, S. (1998). A framework for modelling trojans and computer virus infection. *The Computer Journal*, *41*(7), 444-458.

Tschirhart, J. (2004). A new adaptive system approach to predator-prey modeling. *Ecological Modeling*, *176*(3-4), 255-276.

Vascellaro, J. E., Steel, E., & Adams R. (2011). News Corp. Sells Myspace for a song. *The Wall Street Journa*l. Retrieved from http://www.wsj.com/articles/SB10001424052702304584004576415932273770852

Venkatesh, V., Morris, M., Davis, G., & Davis, F. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*. 27(3), 425-478.

Verizon. (2013). *2013 data breach investigations report*. Retrieved from http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf

Verizon. (2014). *2014 data breach investigations report.* Retrieved from http://www.verizonenterprise.com/resources/reports/rp_Verizon-DBIR-2014_en_xg.pdf

Verzion (2015). *2015 data breach investigations report.* Retrieved from https://msisac.cisecurity.org/whitepaper/documents/1.pdf

Wixom, B. H., & Todd, P. A. (2005). A theoretical integration of user satisfaction and technology acceptance. *Information Systems Research*, *16*(1), 85-102.

Xiang, Y., Zhou, W., & Li, Z. (2006). An analytical model for DDoS attacks and defense. In *Proceedings of the International Multi-Conference on Computing in the Global Information Technology*.

Yadron, D. (2014). Corporate boardrooms race to shore up cybersecurity. *The Wall Street Journal*. Retrieved from http://www.wsj.com/articles/boards-race-to-bolster-cybersecurity-1404086146

Yang, R., Kiekintveld, C., Ordonez, F., Tambe, M., & John, R. (2013). Improving resource allocation strategies against human adversaries in security games: An extended study. *Artificial Intelligence*, *195*, 440-469.

Appendix A: Notation

Table A1. Notation

V	Value of the system
U	Amount of use
A	Number of attacks
$\dot{X}$	Time rate of change of X
Kv	Natural exogenous upper limit on system value
Ku	Natural exogenous upper limit on usage
u0	Value of V at which the upper limit on U is Ku/2
u1	Natural rate at which users quit using the system
u2	Rate at which usage and value increase users
v0	Value of U at which the upper limit on V is Kv/2
v1	Natural “obsolescence” rate of the system values
v2	Rate at which usage and value increases value
v3	Rate at which attacks and value decrease value
a1	Natural rate at which attackers quit attacking
a2	Rate at which attacks and value increase attackers
I	Investment in infrastructure
s	Investment in security

Appendix B: Maple Scripts

Note: Some output and white space has been removed for clarity and some inadvertent reformatting occurred in the transfer from Maple (by Waterloo Maple, Inc.).

```
> ##############Obligate mutualism###### 15 Dec 2015
> restart;interface(warnlevel=0):
> with(plottools):with(plots):with(Student[Calculus1]):with(Student):
> with(VectorCalculus):with(LinearAlgebra):interface(warnlevel=3):
> ################### the differential equations################
> Udot:=-u1*U+u2*U*V*(1-U*(u0+V)/(ku*V)):;
> Vdot:=-v1*V+v2*U*V*(1-V*(v0+U)/(kv*U)):;
      > ######################################################################
> ############################## Section 1 ########################
> ################### the jacobian ##############################
> J:=simplify(Jacobian([Vdot,Udot],[V,U]));
```

$$J := \left[\left[-\frac{2\,U\,V\,v2 - U\,kv\,v2 + 2\,V\,v0\,v2 + kv\,v1}{kv}, -\frac{v2\,V\,(V - kv)}{kv} \right], \left[-\frac{u2\,U\,(U - ku)}{ku}, -\frac{2\,U\,V\,u2 + 2\,U\,u0\,u2 - V\,ku\,u2 + ku\,u1}{ku} \right] \right]$$

```
> ################################nullclines#######################
> eq1:=U*V+v0*V-kv*U+kv*v1/v2=0:
> eq2:=U*V+u0*U-ku*V+ku*u1/u2=0:
> ################################find the critical points########
> ################ intersection of the null clines##############
> intercepts:=(solve({eq1,eq2},{V,U})):eval(radical(intercepts)):;
> intercepts:=(solve({eq1,eq2},{U,V})):eval(radical(intercepts)):;
> ###################SECTION 2 ############################
> ################  PARAMETER SET 1 ######################
> ###################### TABLE 2##################
> ku:=100:kv:=300:
> v0:=20:v1:=.1:v2:=.01:
> u0:=60:u1:=.1:u2:=.01:
> s:=solve({Udot,Vdot},{U,V});   s[1,1];    # find the  critical points
```

$$s := \{U = 12.10124957,\ V = 19.63708205\},\ \{U = 73.45430598,\ V = 203.6962513\}$$

$$U = 12.10124957$$

```
> #!MAGIC NUMBER! to deal with random order of solutions
> Vstar:=203.6962513;
```

$$Vstar := 203.6962513$$

```
> ####################SECTION 3 ####################
> ################### Critical Point Evaluation ##################
> ################  TABLE 3  ################
> intercepts:=evalf(solve({Vdot,Udot},{V,U}));
> V1intercept:=solve({eq1,U=0},{V,U});U1intercept:=solve({eq1,V=0},{V,U});
> V2intercept:=solve({eq2,U=0},{V,U});U2intercept:=solve({eq2,V=0},{V,U});
> Origin:=solve({V=0,U=0},{V,U});
> print("+++++++++++++++++");;
> ##################Jacobian at intersection###################
> intercepts[1];J1:=simplify(eval(J,intercepts[1])); E1:=Eigenvalues(Matrix(J1));
> print("+++++++++++++++++");
> intercepts[2];J2:=eval(J,intercepts[2]);E2:=Eigenvalues(J2);
> print("+++++++++++++++++");;
> Origin;J0:=eval(J,Origin); E0:=Eigenvalues(J0);
> print("+++++++++++++++++");
> U1intercept;J4:=eval(J,U1intercept); E4:=Eigenvalues(J4);
> print("+++++++++++++++++");
> V2intercept;J5:=eval(J,V2intercept); E5:=Eigenvalues(J5);
> print("+++++++++++++++++");
```

$$intercepts := \{U = 12.10124957,\ V = 19.63708205\},\ \{U = 73.45430598,\ V = 203.6962513\}$$

$$V1intercept := \{U = 0.,\ V = -150.\}$$

$$U1intercept := \{U = 10.,\ V = 0.\}$$

$$V2intercept := \{U = 0.,\ V = 10.\}$$

$$U2intercept := \{U = -16.66666667,\ V = 0.\}$$

$$Origin := \{U = 0,\ V = 0\}$$

"+++++++++++++++++"

$$\{U = 12.10124957,\ V = 19.63708205\}$$

$$J1 := \begin{bmatrix} -0.02101249575 & 0.1835169875 \\ 0.1063684716 & -0.09637082044 \end{bmatrix}$$

$$E1 := \begin{bmatrix} 0.08601542786 \\ -0.2033987441 \end{bmatrix}$$

"++++++++++++++++++++"

$$\{U = 73.45430598,\ V = 203.6962513\}$$

$$J2 := \begin{bmatrix} -0.6345430600 & 0.6538904199 \\ 0.1949895531 & -1.936962513 \end{bmatrix}$$

$$E2 := \begin{bmatrix} -0.5430712202 \\ -2.028434353 \end{bmatrix}$$

"++++++++++++++++++++"

$$\{U = 0,\ V = 0\}$$

$$J0 := \begin{bmatrix} -0.1 & 0 \\ 0 & -0.1 \end{bmatrix}$$

$$E0 := \begin{bmatrix} -0.1000000000 \\ -0.1000000000 \end{bmatrix}$$

"++++++++++++++++++++"

$$\{U = 10.,\ V = 0.\}$$

$$J4 := \begin{bmatrix} -0. & 0. \\ 0.09000000000 & -0.2200000000 \end{bmatrix}$$

$$E4 := \begin{bmatrix} 0 \\ -0.2200000000 \end{bmatrix}$$

"++++++++++++++++++++"

$$\{U = 0.,\ V = 10.\}$$

$$J5 := \begin{bmatrix} -0.1133333333 & 0.09666666667 \\ 0. & -0. \end{bmatrix}$$

$$E5 := \begin{bmatrix} -0.1133333333 \\ 0 \end{bmatrix}$$

"++++++++++++++++++++"

> ####################SECTION 4 ######################################

> ################ Plot Nullclines and Phase Portraits ############

> ############################ Figure 2 ########################

> with(DEtools):unassign('ku','kv','v0','v1','v2','u0','u1','u2');

> de1:=diff(U(t),t)=-u1*U(t)+u2*U(t)*V(t)*(1-U(t)*(u0+V(t))/(ku*V(t))):

> de2:=diff(V(t),t)=-v1*V(t)+v2*U(t)*V(t)*(1-V(t)*(v0+U(t))/(kv*U(t))):

> ku:=100:kv:=300:v0:=20:v1:=.1:v2:=.01:u0:=60:u1:=.1:u2:=.01:

> init := V(0)=100,U(0)=100:;

> U1:=solve(eq1,U):U2:=solve(eq2,U):f1:=x->eval(U1,V=x):f2:=x->eval(U2,V=x):

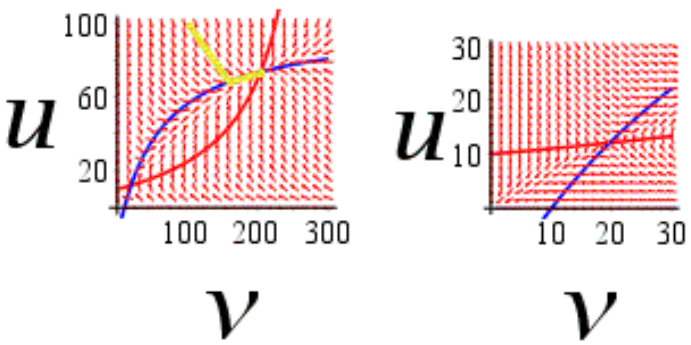
> P1:=plot([f1(v),f2(v)],v=0..300,u=0..100,color=[red,blue],linestyle=[1,1],thickness=[1,1]):

> P2:=plot([f1(v),f2(v)],v=0..30,u=0..30,color=[red,blue],linestyle=[1,1],thickness=[1,1]):

> P3:=phaseportrait({de1,de2},[V(t),U(t)],t=0..100,[[init]],U=0..100,V=0..300,labelfont=["Times",30]):

> P4:=phaseportrait({de1,de2},[V(t),U(t)],t=0..100,[[init]],U=0..30,V=0..30,labelfont=["Times",30]): #close up on unstable CP

> display({P1,P3});display({P2,P4});



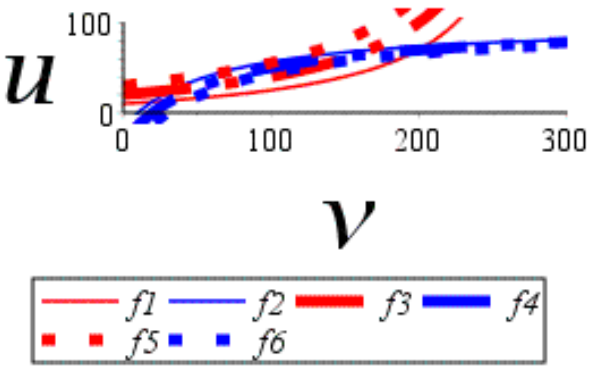
```
> ##########################SECTION 5 ########################
> ################ Sensitivity Analysis ####################
> ###################### Figure 3 ################################
> #######plot nullclines for various values of u1 and v1#########
> ku:=100:kv:=300:
> v0:=20:v1:=.1:v2:=.01:
> u0:=60:u1:=.1:u2:=.01:
> U1:=solve(eq1,U):U2:=solve(eq2,U):f1:=x->eval(U1,V=x):f2:=x->eval(U2,V=x):
> unassign('u1');u1alt1:=.2;:unassign('v1');v1alt1:=.2;
> U3:=subs(v1=v1alt1,subs(u1=u1alt1,[solve(eq1,U)])):
> U4:=subs(v1=v1alt1,subs(u1=u1alt1,[solve(eq2,U)])):
> f3:=x->eval(U3[1],V=x):f4:=x->eval(U4[1],V=x):
> u1alt2:=.3;v1alt2:=.3;
> U5:=subs(v1=v1alt2,subs(u1=u1alt2,[solve(eq1,U)])):
> U6:=subs(v1=v1alt2,subs(u1=u1alt2,[solve(eq2,U)])):
> f5:=x->eval(U5[1],V=x):f6:=x->eval(U6[1],V=x):
> plot([f1(v),f2(v),f3(v),f4(v),f5(v),f6(v)],v=0..300,u=0..100,color=[red,blue,red,blue,red,blue],
linestyle=[1,1,4,4,2,2],thickness=[1,1,5,5,5,5],legend=['f1','f2','f3','f4','f5','f6'],labelfont=["Times",30]);
```

$$u1alt1 := 0.2$$

$$v1alt1 := 0.2$$

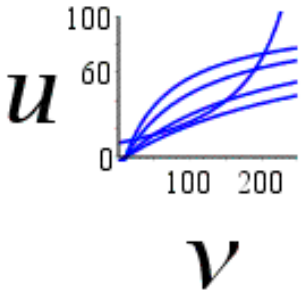
$$u1alt2 := 0.3$$

$$v1alt2 := 0.3$$




```
>
> ################################################
> ###################### Figure 4 ####################
> #### plot nullclines for various value of u0 ###
> ku:=100:kv:=300:
> v0:=20:v1:=.1:v2:=.01:
> u0:=60:u1:=.1:u2:=.01:
```

```
> U1:=solve(eq1,U):U2:=solve(eq2,U):
> u0:=100:U2100:=solve(eq2,U):g2:=x->eval(U2100,V=x):
> u0:=200:U2200:=solve(eq2,U):g3:=x->eval(U2200,V=x):
> u0:=300:U2300:=solve(eq2,U):g4:=x->eval(U2300,V=x):
> fku:=x->ku:fkw(x):=x->kv:fcu:=x->-v0:  #functions for plot
> f:=x->eval(U1,V=x):                    # need for plots
> g:=x->eval(U2,V=x):                    # need for plots
> plot([f(v),g(v),g2(v),g3(v),g4(v)],v=0..250,u=0..100, thickness=2,color=[blue],thickness=[1],labelfont=["Times",30]);
>
```




```
> ################ SECTION 6 ##############################
> ###### RESET PARAMETERS TO CASE 1 #############
> ku:=100:kv:=300:
> v0:=20:v1:=.1:v2:=.01:
> u0:=60:u1:=.1:u2:=.01:
                    > ########## Derivatives of V at the CP near (73,203) ###############
> ######## Calculate with diff function  ########
> ##########   For TABLE 5 ############
> ############ Calculate dVdv1 ############################
> old:=v1;unassign('v1');x:=v1;
> i:=solve(({Udot,Vdot},{V,U})):i:=allvalues(i);
> ## calculate derivatives for both values of V* ##
> cp1:=i[1,2]:d:=diff(%,v1);Vs1:=rhs(evalf(subs(v1=old,cp1))):dV1dx:=evalf(subs(v1=old,d)):
> cp2:=i[2,2]:d:=diff(%,v1);Vs2:=rhs(evalf(subs(v1=old,cp2))):dV2dx:=evalf(subs(v1=old,d)):
> if Vs1>Vs2 then dVdx:=dV1dx; Vx:=Vs1; else dVdx:=dV2dx; Vs:=Vs2; end if;
> v1:=old;
```

$$old := 0.1$$

$$x := v1$$

$$i := \left\{ U = 41.66666667\, v1 + 38.61111111 + 0.2777777777 \sqrt{22500\, v1^2 - 66300\, v1 + 18601}\,, \; V = -125\, v1 + \frac{745}{6} + \frac{5}{6} \sqrt{22500\, v1^2 - 66300\, v1 + 18601} \right\}, \left\{ U = 41.66666667\, v1 + 38.61111111 - 0.2777777777 \sqrt{22500\, v1^2 - 66300\, v1 + 18601}\,, \; V = -125\, v1 + \frac{745}{6} - \frac{5}{6} \sqrt{22500\, v1^2 - 66300\, v1 + 18601} \right\}$$

$$d := 0 = -125 + \frac{5}{12} \frac{45000\, v1 - 66300}{\sqrt{22500\, v1^2 - 66300\, v1 + 18601}}$$

$$d := 0 = -125 - \frac{5}{12} \frac{45000\, v1 - 66300}{\sqrt{22500\, v1^2 - 66300\, v1 + 18601}}$$

$$dVdx := 0. = -358.1677735$$

$$Vx := 203.6962513$$

$$v1 := 0.1$$

> ##################Check by perterbation######

> delta:=0.00001;old:=v1;v1:=old+delta;

> i:=solve(({Udot,Vdot},{V,U}));:

> Vstar1:=rhs(i[1,2]):Vstar2:=rhs(i[2,2]):

> Vnew:=max(Vstar1,Vstar2);

> dVdv1:=(Vnew-Vstar)/delta;v1:=old;

$$\delta := 0.00001$$

$$old := 0.1$$

$$v1 := 0.10001$$

$$i := \{U = 12.10244347,\ V = 19.63816375\},\ \{U = 73.45394542,\ V = 203.6926696\}$$

$$Vnew := 203.6926696$$

$$dVdv1 := -358.17$$

$$v1 := 0.1$$

> ############# Calculate dVdv2 ############################

> old:=v2;unassign('v2');x:=v2;

> i:=solve(({Udot,Vdot},{V,U})):i:=allvalues(i):;

> cp1:=i[1,2]:d:=diff(%,v2):Vs1:=rhs(evalf(subs(v2=old,cp1))):dV1dx:=evalf(subs(v2=old,d)):

> cp2:=i[2,2]:d:=diff(%,v2):Vs2:=rhs(evalf(subs(v2=old,cp2))):dV2dx:=evalf(subs(v2=old,d)):

> if Vs1>Vs2 then dVdx:=dV1dx; Vx:=Vs1; else dVdx:=dV2dx; Vs:=Vs2; end if;

> v2:=old;

$$old := 0.01$$

$$x := v2$$

$$dVdx := 0. = 3581.67773$$

$$Vx := 203.6962513$$

$$v2 := 0.01$$

> ##################Check by perterbation######

> old:=v2;v2:=old+delta;

> i:=solve(({Udot,Vdot},{V,U})):;

> Vstar1:=rhs(i[1,2]):Vstar2:=rhs(i[2,2]):

> Vnew:=max(Vstar1,Vstar2);

> dVdv2:=(Vnew-Vstar)/delta;v2:=old;

$$old := 0.01$$

$$v2 := 0.01001$$

$$Vnew := 203.7320302$$

$$dVdv2 := 3577.89$$

$$v2 := 0.01$$

> ################ Calculate dVdu1 ##########################

> old:=u1;unassign('u1');x:=u1;

> i:=solve(({Udot,Vdot},{V,U})):i:=allvalues(i):;

> cp1:=i[1,2]:d:=diff(%,u1):Vs1:=rhs(evalf(subs(u1=old,cp1))):dV1dx:=evalf(subs(u1=old,d)):

> cp2:=i[2,2]:d:=diff(%,u1):Vs2:=rhs(evalf(subs(u1=old,cp2))):dV2dx:=evalf(subs(u1=old,d)):

> if Vs1>Vs2 then dVdx:=dV1dx; Vx:=Vs1; else dVdx:=dV2dx; Vs:=Vs2; end if;

> u1:=old;

$$old := 0.1$$

$$x := u1$$

$$dVdx := 0. = -43.60180712$$

$$Vx := 203.6962513$$

$$u1 := 0.1$$

> ########Check by perterbation#################

> old:=u1;u1:=old+delta;

> i:=solve(({Udot,Vdot},{V,U})): #solve for CP as a function of u1

> Vstar1:=rhs(i[1,2]):Vstar2:=rhs(i[2,2]):

> Vnew:=max(Vstar1,Vstar2):;

> dVdu1:=(Vnew-Vstar)/delta;u1:=old;

$$old := 0.1$$

$$u1 := 0.10001$$

$$dVdu1 := -43.60$$

$$u1 := 0.1$$

> ############ Calculate dVdu2 ############################

> old:=u2;unassign('u2');x:=u2;

> i:=solve(({Udot,Vdot},{V,U})):i:=allvalues(i):;

> cp1:=i[1,2]:d:=diff(%,u2):Vs1:=rhs(evalf(subs(u2=old,cp1))):dV1dx:=evalf(subs(u2=old,d)):

> cp2:=i[2,2]:d:=diff(%,u2):Vs2:=rhs(evalf(subs(u2=old,cp2))):dV2dx:=evalf(subs(u2=old,d)):

> if Vs1>Vs2 then dVdx:=dV1dx; Vx:=Vs1; else dVdx:=dV2dx; Vs:=Vs2; end if;

> u2:=old;

$$old := 0.01$$

$$x := u2$$

$$dVdx := 0. = 436.01807$$

$$Vx := 203.6962513$$

$$u2 := 0.01$$

>

> ##################Check by perterbation######

> delta:=.000001;old:=u2;u2:=old+delta;

> i:=solve(({Udot,Vdot},{V,U})):

> Vstar1:=rhs(i[1,2]):Vstar2:=rhs(i[2,2]):

> Vnew:=max(Vstar1,Vstar2);

> dVdu2:=(Vnew-Vstar)/delta;u2:=old;

$$\delta := 0.000001$$

$$old := 0.01$$

$$u2 := 0.010001$$

$$Vnew := 203.6966873$$

$$dVdu2 := 436.0$$

$$u2 := 0.01$$

>

> ############ Calculate dVdkv ############################

> delta:=.00001;old:=kv;unassign('kv');x:=kv;

> i:=solve(({Udot,Vdot},{V,U})):i:=allvalues(i):;

> cp1:=i[1,2]:d:=diff(%,kv):Vs1:=rhs(evalf(subs(kv=old,cp1))):dV1dx:=evalf(subs(kv=old,d)):

> cp2:=i[2,2]:d:=diff(%,kv):Vs2:=rhs(evalf(subs(kv=old,cp2))):dV2dx:=evalf(subs(kv=old,d)):

> if Vs1>Vs2 then dVdx:=dV1dx; Vx:=Vs1; else dVdx:=dV2dx; Vs:=Vs2; end if;

> kv:=old;

$$\delta := 0.00001$$

$$old := 300$$

$$x := kv$$

$$dVdx := 0. = 0.7575762496$$

$$Vx := 203.6962513$$

$$kv := 300$$

> ##################Check by perterbation######

> old:=kv;kv:=old+delta;

> i:=solve(({Udot,Vdot},{V,U})):

> Vstar1:=rhs(i[1,2]):Vstar2:=rhs(i[2,2]):

> Vnew:=max(Vstar1,Vstar2);

> dVdkv:=(Vnew-Vstar)/delta;kv:=old;

$$old := 300$$

$$kv := 300.00001$$

$$Vnew := 203.6962589$$

$$dVdkv := 0.76$$

$$kv := 300$$

> ############ Calculate dVdku ############################

> old:=ku;unassign('ku');x:=ku;

> i:=solve(({Udot,Vdot},{V,U})):i:=allvalues(i):;

> cp1:=i[1,2]:d:=diff(%,ku):Vs1:=rhs(evalf(subs(ku=old,cp1))):dV1dx:=evalf(subs(ku=old,d)):

> cp2:=i[2,2]:d:=diff(%,ku):Vs2:=rhs(evalf(subs(ku=old,cp2))):dV2dx:=evalf(subs(ku=old,d)):

```
> if Vs1>Vs2 then dVdx:=dV1dx; Vx:=Vs1; else dVdx:=dV2dx; Vs:=Vs2; end if;
> ku:=old;
```

$$old := 100$$

$$x := ku$$

$$dVdx := 0. = 0.8445506591$$

$$Vx := 203.6962513$$

$$ku := 100$$

```
>> ##################Check by perterbation######
> old:=ku;ku:=old+delta;
> i:=solve(({Udot,Vdot},{V,U})):;
> Vstar1:=rhs(i[1,2]):;
> Vstar2:=rhs(i[2,2]):;
> Vnew:=max(Vstar1,Vstar2);
> dVdku:=(Vnew-Vstar)/delta;ku:=old;
```

$$old := 100$$

$$ku := 100.00001$$

$$Vnew := 203.6962597$$

$$dVdku := 0.84$$

$$ku := 100$$

```
#############################################################
                        ### 3D Model ##
#############################################################
> #### 3 species 3d solution with no upper bound on A
> restart; with(VectorCalculus):with(student):with(LinearAlgebra):
> # 18 May 2015,
> # revised 17 Aug 2015, 15 Dec 2015
> ########## the 3d differential equations###################
> Vdot:=v2*U*V*(1-V*(v0+U)/(kv*U)) - v3*A*V:
> Udot:=-u1*U+u2*U*V*(1-U*(u0+V)/(ku*V)):
> Adot:=-a1*A+a2*A*V:
> ########################## 3d nullclines################
> eqV:=U*V+v0*V-kv*U +kv*v1/v2+A*kv*v3/v2=0:
> eqU:=U*V+u0*U-ku*V+ku*u1/u2=0:
> eqA:=-a1+a2*V=0:
> Astar:=solve(eqA,V):
> Ustar:=subs(V=a1/a2,solve(eqU,U)):
> Astar:=solve(subs(V=a1/a2,subs(U=ku*(+V*u2-u1)/(u2*(u0+V)),eqV)),A):
```

```
> ################### 3d jacobian#########################
> J3d:=Jacobian([Vdot,Udot,Adot],[V,U,A]):
> J3d:=subs(V=a1/a2,subs(U=ku*(+V*u2-u1)/(u2*(u0+V)),J3d)):
> ############### prep nullclines for plotting #########
> eq1V:=solve(eqV,V):eq2V:=solve(eqU,V):eq3V:=solve(eqA,V):
> ## 3d plot prep ######################
> plotncV:=(x,y)->eval(eq1V,{U=x,A=y}):
> plotncU:=(x,y)->eval(eq2V,U=x):
> plotncA:=(x,y)->eval(eq3V,A=y):
> ######################### CASE 1 ############################
> kv:=30000;ku:=10000;
> v0:=100;v1:=0.001;v2:=.03;v3:=.1;
> u0:=100;u1:=.01;u2:=.01;
> a1:=.1;a2:=.00001;
> fku:=x->ku:fkv(x):=x->kv:fcu:=x->-v0:fav:=y->u0:
```

$$kv := 30000$$

$$ku := 10000$$

$$v0 := 100$$

$$v1 := 0.001$$

$$v2 := 0.03$$

$$v3 := 0.1$$

$$u0 := 100$$

$$u1 := 0.01$$

$$u2 := 0.01$$

$$a1 := 0.1$$

$$a2 := 0.00001$$

```
> ################ SECTION 7 ##############################
> ################### Existence of Various Responses ##########
> ###############################################
> ##### Table 7 Case 4 &  Equation 16 Jacobian #####
> a2:=.00001;cp3d:=solve({eqA,eqU,eqV});
> j3d:=Matrix(eval(J3d,cp3d));E:=evalf(Eigenvalues(j3d));
```

$$a2 := 0.00001$$

$$cp3d := \{A = 1969.990000,\ U = 9900.,\ V = 10000.\}$$

$$j3d := \begin{bmatrix} -99.9990000 & 200.0000000 & -1000.000000 \\ 0.9900000000 & -99.99000000 & 0 \\ 0.01969990000 & 0 & 0 \end{bmatrix}$$

$$E := \begin{bmatrix} -113.979567170592 + 0.\,I \\ -85.8080299592548 + 0.\,I \\ -0.201402870153061 + 0.\,I \end{bmatrix}$$

> ###################### Table 7 Case 5 ########################

> a2:=.00006;cp3d:=solve({eqA,eqU,eqV});

> j3d:=Matrix(eval(J3d,cp3d)):E:=evalf(Eigenvalues(j3d));

$$a2 := 0.00006$$

$$cp3d := \{A = 2669.675535,\ U = 9428.301887,\ V = 1666.666667\}$$

$$E := \begin{bmatrix} -31.8232176491494 + 0.\,I \\ -0.356476060425268 + 3.72106672401420\,I \\ -0.356476060425268 - 3.72106672401420\,I \end{bmatrix}$$

> ###################### Table 7 Case 6 ########################

> a2:=.001;cp3d:=solve({eqA,eqU,eqV});

> j3d:=Matrix(eval(J3d,cp3d));E:=evalf(Eigenvalues(j3d));

> EigenVectors:=evalf(Eigenvectors(j3d, output='list')):;

$$a2 := 0.001$$

$$cp3d := \{A = 1479.940000,\ U = 4950.,\ V = 100.\}$$

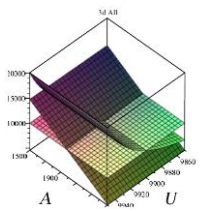
$$j3d := \begin{bmatrix} -0.5040000 & 2.990000000 & -10.00000000 \\ 24.99750000 & -0.9900000000 & 0 \\ 1.479940000 & 0 & 0 \end{bmatrix}$$

$$E := \begin{bmatrix} -8.60227688443876 + 0.\,I \\ 6.85999674760145 + 0.\,I \\ 0.248280136837326 + 0.\,I \end{bmatrix}$$

> ################## SECTION 8 ##############################

> ############## 3d Nullcines ##############

> ##



> umin:=9850:umax:=9950:amin:=1500:amax:=2500:a2:=.00001;

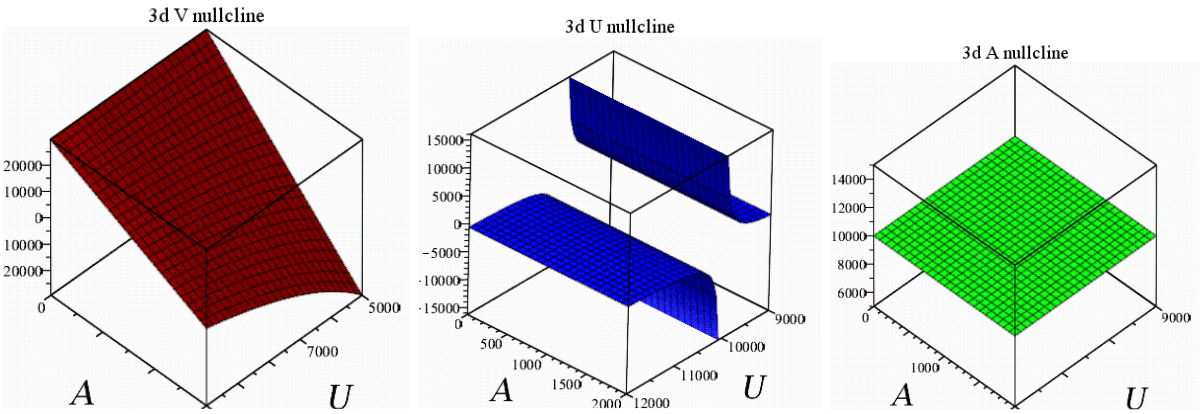
> plot3d({plotncV(u,a), plotncU(u,a), plotncA(u,a)},u=umin..umax,a=amin..amax, axes=boxed, title="3d All");

$$a2 := 0.00001$$

> ##

> ############## Individual Nullcines ##############

```
> ##########################################################
> umin:=5000:umax:=10000:amin:=0:amax:=3000:
> plot3d(plotncV(u,a),u=umin..umax,a=amin..amax, color=(red), labels = ['U','A','V'],axes=boxed, title="3d V nullcline",titlefont=[TIMES,ROMAN,16],labelfont=["Times",25]);
> umin:=9000:umax:=12000:amin:=0:amax:=2000:
> plot3d(plotncU(u,a),u=umin..umax,a=amin..amax, color=(blue), labels = ['U','A','V'],axes=boxed, titlefont=[TIMES,ROMAN,16],title="3d U nullcline",titlefont=[TIMES,ROMAN,16],labelfont=["Times",25]);
> plot3d(plotncA(u,a),u=umin..umax,a=amin..amax, color=(green), axes=boxed, labels = ['U','A','V'],title="3d A nullcline",titlefont=[TIMES,ROMAN,16],labelfont=["Times",25]);
>
```



Appendix D: ODEToolkit Setup for Figure 8

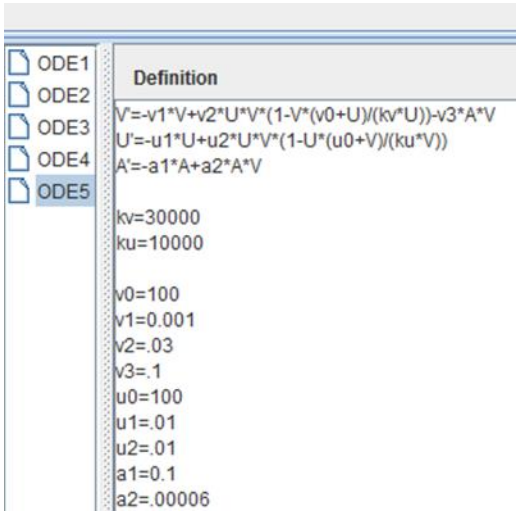


Figure D1. ODEToolkit Setup for Figure 8

About the Author

Norman Pendegraft is Professor of Management Information Systems at the College of Business and Economics at the University of Idaho. His teaching interests include analytics, relational and nosql database design, and fencing. His major research interest is the economics of information system security.

JITTA

JOURNAL OF INFORMATION TECHNOLOGY THEORY AND APPLICATION

JITTA is a Publication of the Association for Information Systems
ISSN: 1532-3416